Research Paper Computer Science

Local Ends Cryptography

* CRS BHARDWAJ

* 33, first floor, BDA layout, HAL IInd stage, Kodihalli, 6th main, Bangalore

ABSTRACT

This research paper discusses the Local Ends Cryptography which is associated with the local modification of the message before the transmission to ensure the safety, security and confidential exchange of information. In this era cryptography where number of stations has sophisticated software to decipher the message it is not possible to exchange the message safely. Therefore before sending the message by the commercial Standard encryption techniques it is encrypted by using the local cryptography which is known to the individuals. Local ends cryptography is helpful because of software are available to decipher the message during the transitions. The modified encryption of data locally cannot be deciphered by the standard software which is easily available in the market. It enables you to send the secure data between two computers on private wireless link and lines.

Keywords : wireless link, local end cryptography, encryption, commercial, software

Introduction

In this golden era of communications, everything depends on the secrecy of the communications. Online data communications are basis of the progress of a person or an organization. The cyber security plays a crucial and critical role in modern times for businesses and in the military wars. The information which is passed on the Internet for commercial purposes is confidential. During the wars and trades, only those get success that uses the confidential information system. To cater these security issues, various Symmetric-key and asymmetric-key type security protocols have been developed. In this paper, Local Ends Cryptography has been explained which is based on the fact that till you have something secret in your hand, it can be leak anywhere in the middle during the transmission.

Symmetric-key encryption techniques Symmetric-key algorithms[1] are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. Examples of popular and well-respected symmetric algorithms include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, RC4, 3DES, and IDEA.

Asymmetric key encryption techniques

There are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. Various asymmetric encryption algorithms (RSA, Elgamal) have been implemented [5].

Pretty good privacy (pgp)

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications. Current versions of PGP encryption include both options through an automated key management server [6].

Materials, apparatus and procedures

No any method of encryption is secure as it has also decoding software. Once it is traced your information can be decoded by your enemy. Till the information is not in your hand it can be leaked out certainly. If you are the first and last man to decode the information then sourly you will get through. You will not get the chance to repeat your mistakes. Before transmission of the message it should be encrypted locally by using the local techniques. Let us to encrypt the message 'Bhardwaj'. It can be encrypted by using many techniques. The encryption of 'Bhardwaj' may be "cibsexbk". This encryption can be obtained by shifting every letter towards right by one place. Some methods of local cryptography are given below.

Method 1:- We can interchange the first and last letter of every word before the transmission of any messages. After local cryptography the message can be transmitted by using any crypto software.

Bhardwaj = {1, 7, 0, 17, 3, 22, 0, 9}, (interchange the first and the last digit) {9, 7, 0, 17, 3, 22, 0, 1} = [j, h, a, r, d, w, a, b]

Plain text: Bhardwaj

Key: Interchange the first and last letter of every word.

Cipher Text: jhardwab (convert this text into numbers 9, 7, 0, 17, 3, 22, 0, 1)

Method 2:- We can change the text into numbers and then add one to each digit to modify the message before transmission. After reception the process can be reversed to get the plain text. Plain text: Bhardwaj

Key: add one to each digit

Cipher Text: {2, 8, 1, 18, 4, 23, 1, 10} = [c, i, b, s, e, x, b, k]

Method 3:- We can change the text into numbers and then subtract one from each digit to modify the message before transmission. After reception the process can be reversed to

get the plain text.

Plain text: Bhardwaj

Key: subtract one from each digit

Cipher Text: {0, 6, 25, 16, 2, 21, 25, 8} = [a, g, z, q, c, v, z, i]

Method 4:- Plain text can be changed into numbers and the key can be thought separately according to the suitability of the situation and then the key numbers can be added to the plain text message and then find the remainder by dividing it by the number twenty five to modify the message before transmission.

Text = Bhardwaj = {1, 7, 0, 17, 3, 22, 0, 9}

Key = Bhardwaj = {1, 7, 0, 17, 3, 22, 0, 9}

Cipher text = {2, 14, 0, 34, 6, 44, 0, 18} (add the key to the text mod 25) {c, n, a, j, g, t, a, s}

Method 5:- Plain text can be changed into numbers and the key can be thought separately according to the suitability of the situation and then the key numbers can be subtracted from the plain text message and then find the remainder by dividing it by the number twenty five to modify the message before transmission.

Text = Bhardwaj {1, 7, 0, 17, 3, 22, 0, 9}

Key = Bhardwaj {1, 7, 0, 17, 3, 22, 0, 9}

Cipher text = {0, 0, 0, 0, 0, 0, 0, 0} (subtract the key from the text) {a, a, a, a, a, a ,a ,a}

Method 6:- Plain text can be changed into numbers and the key can be thought separately according to the suitability of the situation and then the key numbers can be multiplied to the plain text message numbers and then find the remainder by dividing it by the number twenty five to modify the message before transmission.

Text = Bhardwaj {1, 7, 0, 17, 3, 22, 0, 9}

Key = Bhardwaj {1, 7, 0, 17, 3, 22, 0, 9}

Cipher text = {1, 49, 0, 289, 9, 484, 0, 81} (multiply the key with the text mod 25) {b, y, a, o, j, j, a, g}

Method 7:- There are twenty six letters from zero to twenty five. Plain text can be modified by subtracting the number from twenty five before transmission and adding twenty five during the reception of text. It means that the receiving text is the conjugate of the transmitting text.

Text = Bhardwaj {1, 7, 0, 17, 3, 22, 0, 9}

Key = 25

Cipher text = {24, 18, 25, 8, 22, 3, 25, 16} (subtract the number of the plain text from twenty five) {y, s, z, i, w, d, z, q}

Method 8:- The two letters of the plain text can be interchanged to cipher the text. After reception the process can be reversed to get the plain text. After local cryptography the message can be transmitted by using any crypto software.

Text = Bhardwaj {1, 7, 0, 17, 3, 22, 0, 9}

Key = interchanged the letters

Cipher text = {7, 1, 17, 0, 22, 3, 9, 0} {h, b, r, a, w, d, j, a}

Method 9:- The plain text can also be ciphered by sending every letter in the group of four or five letters. The message can be hiding at any place of four letters. In the group of four letters the second one is the plain text message).

Text = Bhardwaj {1, 7, 0, 17, 3, 22, 0, 9}

Key = any group of four letters

Cipher text = {(m, b, n, i), (l, h, c, and g), (h, a, t, q), (m, r, d, and f)…….}

Implementation: - The implementation means to install the software. In local end cryptography there is not the requirement of the software. The technique can be prepared well in advance to train the manpower. These technologies can also wok in the adverse condition when the commercial links are in the jammer scan or direction finder scan.

Discussion:

The local ends cryptography is superior than the other commercial methods because is known to the ends only. The symmetrical encryption can be used because it is more than one hundred time faster than Asymmetric Encryption.

The distribution of key is not required as peers communication is used during the war. One message can be transmitted on the complete network. The key can be distributed well in advance. The problem of distributing keys is solved because the codes are prepared locally. Password may be changed daily by referring the serial numbers of the booklet.

Symmetric keys are subject to a brute force attack where all keys in the key space are tried systematically to break the encryption. As we are using local ends cryptography, there is no chance to pick up the actual signals during the transmission by the intruders.

This is the standard protocol that exchange of key is done face to face for one to one communication. One booklet may contain passwords for one month. After one month another booklet of password is issued.

The local end cryptography can also be used to pass the message on telephone lines and on the radio nets. Mobiles services can also be used during the war because the actions are taken very quickly within one hour.

The local end cryptography is very important during the wars where each message has its own value. It is also important in business transactions.

Limitations

1. Using local ends Cryptography can be a complex process because the message is still in the cipher form. The proper person is required to decipher the message.
2. The parties at the terminal ends must be able to use local end Cryptography. It is impossible to use local ends Cryptography unless people at both ends are capable of using this.

Conclusion

This research paper discusses the local ends cryptography which is the science of data encryption, a technology that provides for a safe, secure, and private information exchange. If you want secrecy then only two persons should be involved in the communication. If the message is known end to end then there is no problem at all. The commercial cryptography is not successful as everybody has got the software. Some radio sets can automatically search the stations and then convert it into plain text. It enables you to send the secure data between two computers on private wireless link. Local ends cryptography ensures user authentication, bandwidth sharing, and security from eavesdropping and immunity to interference, and difficulty in detection.

REFERENCES

1. Delfs, Hans & Knebl, Helmut (2007)."Symmetric-key encryption". | 2. Belfield, R. (2007). The Six Unsolved Ciphers: | 3. Diffie, W., & Landau, S. (1998). Privacy on the Line. Boston: MIT Press. | 4. Electronic Frontier Foundation. (1998). | 5. Federal Information Processing Standards (FIPS) 140-2. (2001, May 25). |