Network Security with Cryptography and Steganography

Mrs. N. Dhivya
Assistant Professor,
Department of Computer Science and Applications,
Vivekanandha College of Arts and Sciences for Women
(Autonomous)

Mrs S. Banupriya
Assistant Professor,
Department of Computer Science and Applications,
Vivekanandha College of Arts and Sciences for Women
(Autonomous)

Abstract:- **Network security , cryptography &steganography is the concept to product data while transmitting over the wireless internet and network. It deal with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities. Secure communication refers to the scenario where the message or data shared between two parties can't be accessed by malicious entity. Cryptography provide some of security services for protecting data in network. Steganography is an attempts to achieve secure and undetectable communication**

Key: Network security, types of cryptography, setganography

INTRODUCTION:

Network security is consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. Network can be private, such as within a company, and others which might be open to public access. It involves authorization of data n the network, which is controlled by network administrator. **Cryptography** is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions. Steganography is a method of hiding secret data, by embedding it into an audio, video, image or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.

NETWORK SECURITY:

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats. Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

TYPES OF NETWORK SECURITY DEVICES

Active Devices: These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

Passive Devices

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

Preventative Devices

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

Unified Threat Management (UTM)

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

Firewalls

A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.

Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.

Most personal computers use software-based firewalls to secure data from threats from the internet. Many routers that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.

Firewalls are commonly used in private networks or *intranets* to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

An ideal firewall configuration consists of both hardware and software based devices. A firewall also helps in providing remote access to a private network through secure authentication certificates and logins.

Hardware and Software Firewalls
Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks − e.g., for business purpose − business networking firewall solutions are available.

Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

Antivirus
An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

Content Filtering
Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping and job related contents.

Content filtering can be divided into the following categories −

- Web filtering
- Screening of Web sites or pages
- E-mail filtering
- Screening of e-mail for spam
- Other objectionable content

Intrusion Detection Systems
Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them.

Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage. Intrusion detection systems can also perform the following actions −

- Correct Cyclic Redundancy Check (CRC) errors
- Prevent TCP sequencing issues
- Clean up unwanted transport and network layer options

CRYPTOGRAPHY:

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Consider two parties U1 and U2. Now, U1 wants to send a message m to U2 over a secure channel. So, what happens is as follows. The sender’s message or sometimes called the Plaintext, is converted into an unreadable form using a Key k. The resultant text obtained is called the Ciphertext. This process is known as Encryption. At the time of receival, the Ciphertext is converted back into the plaintext using the same Key k, so that it can be read by the receiver. This process is known as Decryption.
U1 (Sender) U2 (Receiver)
C = E (m, k) ----> m = D (C, k)

Here, C refers to the Ciphertext while E and D are the Encryption and Decryption algorithms respectively.

Let’s consider the case of Caesar Cipher or Shift Cipher as an example. As the name suggests, in Caesar Cipher each character in a word is replaced by another character under some defined rules. Thus, if A is replaced by D, B by E and so on. Then, each character in the word would be shifted by a position of 3. For example:
Plaintext : Geeksforgeeks
Ciphertext : Jhhnvirujhhnv

TECHNIQUES USED FOR CRYPTOGRAPHY:

In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

FEATURES OF CRYPTOGRAPHY ARE AS FOLLOWS:

1. **Confidentiality:**
   Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:**
   Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:**
   The creator/sender of information cannot deny his or her intention to send information at later stage.
4. **Authentication:**
   The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

TYPES OF CRYPTOGRAPHY:

In general there are three types Of cryptography:

1. ***Symmetric Key Cryptography:***
   It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

2. ***Hash Functions:***
   There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

3. ***Asymmetric Key Cryptography:***
   Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

STEGNOGRAPHY

Steganography is a technique of hiding the communication by concealing the secret message into a fake message. The term steganography has Greek influences which means *"covered writing"*. The main idea behind the steganography is to prevent the suspicion about the existence of the information.

The steganography technique involves a cover carrier, secret message, stego key and stego carrier. Text, audio, image and video behaves as cover carriers which contain the hidden information embedded in it. Stego carrier is generated using a cover carrier and embedded message. Stego key is also used as supplementary secret information like a password used by the recipient to extract the message.

FORMS OF STEGANOGRAPHY –

Text: In this steganography, the text can be used as a cover media. To hide the message a word or line can be shifted; whitespaces can be used, even the number and position of the vowels are utilised to conceal the secret message.

Audio: Audio stenography can conceal the secret message in the audio file with the help of its digital representation. It can be achieved easily as a typical 16-bit file has 216 sound levels, and a few levels difference could not be detectable by the human ear.

Video: Video steganography brings more possibilities of disguising a large amount of data because it is a combination of image and sound. Therefore, image and audio steganography techniques can also be employed on the video.

Image: It is the most pervasively used form of steganography, the reason behind this is that it causes least suspicion.

The main disadvantage of using the steganography is a significant amount of overhead it produces for hiding a small amount of information. Additionally, the system must not be discovered otherwise it is useless.

CONCLUSION

Cryptography is a method of preventing the information and communications through the use of codes so that we can protect our data from hackers. The information is intended can read and process it. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing."Steg. Steganography is the process of hiding secret data. Thus the techniques steganography and cryptography techniques are very useful in hiding the data from hackers.

REFERENCE

[1] Predictions and Trends for Information, Computer and Network Security [Online] available: http://www.sans.edu/research/securitylaboratory/article/2140
[2] A White Paper, Securing the Intelligent Network powered by Intel Corporation. [3]. Network Security [Online] available: http://en.wikipedia.org/wiki/Network_security.
[3] Network Security: History, Importance, and Futurel, University of Florida Department of Electrical and Computer Engineering, Bhavya Daya.
[4] Ateeq Ahmad, ―Type of Security Threats and its Prevention", Ateeq Ahmad, Int.J.Computer Technology & Applications, Vol 3 (2), 750-752.

[5] Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257
[6] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks‌l, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.
[7] Network Security Types of attacks [Online] available:http://computernetworkingnotes.com/netw ork-security-access-lists-standards-and extended/types-of-attack.html.
[8] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May2008.
[9] Securing the Intelligent Network [Online] available: http://www.trendmicro.co.in/cloudcontent/us/pdfs/security-intelligence/whitepapers/wp_idc_network-overwatch-layer_threatmngmt.
[10] Hayatle O., Youssef A., Otrok H. Dempster-Shafer Evidence Combining for Anti-Honeypot Technologies. Inf. Sec. J.: A Global Perspective 21, 6 (January 2012), 2012, pp. 306-316. DOI: 10.1080/19393555.2012.738375.
[11] Laurén S., Leppänen V., Rauti S., Uitto J. A Survey on Anti-honeypot and Anti-introspection Methods. Recent Advances in Information Systems and Technologies - Volume 2, WorldCIST'17, Porto Santo Island, Madeira, Portugal, April 11-13, 2017, pp. 125-134. DOI: 10.1007/978-3- 319-56538-5_13.
[12] Markov A.S., Tsirlov V.L. Guidelines for Cybersecurity in the Context of ISO 27032, Voprosy kiberbezopasnosti [Cybersecurity issues], 2014, No 1 (2). P. 28-35. DOI: 10.21681/2311-3456-2014-1-28-35.
[13] Achleitner S., La Porta T., McDaniel P., Sugrim S., Krishnamurthy S.V., Chadha R. Cyber Deception: Virtual Networks to Defend Insider Reconnaissance. In Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats (MIST '16). ACM, New York, NY, USA, 2016, pp. 57-68. DOI: 10.1145/2995959.2995962.
[14] De Gaspari F., Jajodia S., Mancini L.V., Panico A. AHEAD: A New Architecture for Active Defense. In Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig '16). ACM, New York, NY, USA, 2016, pp. 11-16. DOI: 10.1145/2994475.2994481.
[15] Shaw T., Arrowood J., Kvasnicka M., Taylor S., Cook K., Hale J. POSTER: Evaluating Reflective Deception as a Malware Mitigation Strategy. In Proceedings of the 2017 .