Available online at: http://www.advancedscientificjournal.com
http://www.krishmapublication.com
IJMASRI, Vol. 1, issue 1, pp.262-265, Apr. -2025
https://doi.org/10.53633/ijmasri

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY ADVANCED SCIENTIFIC RESEARCH AND INNOVATION (IJMASRI)

ISSN: 2582-9130 IBI IMPACTFACTOR 1.5 DOI: 10.53633/IJMASRI

RESEARCH ARTICLE

NETWORK SECURITY WITH CRYPTOGRAPHY AND STEGANOGRAPHY

Vijayalakshmi M[1] Dharshini A[2] and Selvam S[3]
[1,2,3] *PG & Research Department of Computer Science, St. Ann's College of Arts and Science, Tindivanam -604 001*

Abstract

Network security, cryptography, and steganography refer to the concept of protecting data when it is transmitted over a wireless internet or network. It is concerned with establishing and analyzing protocols that prevent harmful third parties from obtaining information shared between two entities. Secure communication is the scenario in which a message or data shared between two parties cannot be accessed by a malevolent entity. Cryptography provides various security services to protect data in a network. Steganography aims to produce safe and undetected communication.

Keywords: Network security, kinds of cryptography and setganography

Introduction

Network security refers to the policies and practices used to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and its available resources. Some networks are private, such as those within a firm, while others are public. It entails data permission over a network, which is managed by a network administrator. These devices scan the networks and identify potential security pro Cryptography is a means of securing information and communications by using codes to ensure that only the intended recipients can read and comprehend the information. In cryptography, the strategies used to protect information are obtained from mathematical principles and a series of rule- based calculations known as algorithms to change signals in ways that make them difficult to decode.

NETWORK SECURITY:

Network security protects a network from unwanted access and threats. It is the responsibility of network administrators to implement preventive steps to safeguard their networks from potential security risks. Computer networks used for frequent transactions and communication inside the government, people, or businesses require security. The most popular and easiest method of safe guarding a network resource is to give it a unique name and accompanying password.

TYPES OF NETWORK SECURITY DEVICES

Active Devices: These security devices prevent excessive traffic. Examples of such equipment include firewalls, antivirus scanners, and content filtering devices.

Passive Devices

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

Preventative Devices

These devices monitor networks and detect potential security threats. These devices scan networks to identify potential security issues.

Examples include penetration testing equipment and vulnerability assessment appliances.

Unified Threat Management (UTM)

These devices function as all – in –one security gadgets. Examples include firewalls, content screening, web caching, and so on.

Firewalls

A firewall is a network security device that manages and regulates network traffic according to specific protocols. A firewall creates a barrier between a trusted internal network and the internet.

Firewalls are available in both software-based and hardware-based configurations. Hardware-based firewalls can also operate as a network's DHCP server.

Most personal computers utilize software-based firewalls to protect their data from online threats. Many routers that transport data between networks include fire wall components, and many fire walls can perform basic routing duties.

Firewalls are often used in private networks and intranets to prevent illegal internet access. Every message that enters or exits the network is routed through the firewall and inspected for security measures.

An effective firewall configuration includes both hardware and software – based devices. A fire wall also aids in allowing remote access to a private network by utilizing secure authentication certificates and logins.

Hardware and Soft ware Firewalls

Hardware firewalls are standalone products. These are also used in broadband routers. Most hardware firewalls include at least four network ports for connecting other computers. There are firewall solutions available for bigger networks, such as those used for corporate purposes.

Antivirus

An antivirus is a tool for detecting and removing dangerous malware. It was originally intended to detect and eliminate viruses from computers.

Modern antivirus software protects against worms, Trojan horses, adware, spyware, key loggers, and other threats in addition to viruses. Some programs additionally offer protection against malicious URLs, spam, phishing attacks, botnets, and DDoS attacks.

Content Filtering

Unpleasant and offensive emails or web pages are screened by content filtering systems. These are utilized as part of corporate firewalls and personal computers. When someone attempts to access an unauthorized web page or email, these devices display the message "Access Denied".

Pornographic content is typically reviewed, as is content that is violent or hateful. Organizations also eliminate shopping and job-related content.

Intrusion Detection Systems

- Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are appliances that monitor malicious network activity, log information about it, take action to stop it, and finally report it.
- Intrusion detection systems assist in issuing an alarm against any malicious behaviour in the network, dropping packets, and resetting the connection to protect the IP address from

blockages. Intrusion detection systems can conduct the following actions:

- Corrected Cyclic Redundancy Check (CRC) errors. Avoid TCP sequencingdifficulties. Remove unneeded transport and network layer choices.

CRYPTOGRAPHY:

Cryptography is a technique for safe guarding information and communications by using codes that only the intended recipients can understand and interpret. This prevents unauthorized access to data. The word "crypt" means "hidden" and the suffix graphy means "writing".

Cryptography techniques used to safeguard information are derived from mathematical ideas and a set of rule-based calculations known as algorithms to modify signals in ways that make them difficult to decode. These algorithms are used to generate cryptographic keys, perform digital signature and verification to safeguard data privacy, browse the internet, and protect secret transactions such as credit card and debit card transactions.

TECHNIQUES USED FOR CRYPTOGRAPHY:

In today's computer age, cryptography is commonly connected with the process of converting regular plain text tocipher text, which is text that can only be decoded by the intended receiver of the text, and so this process is known as encryption. Decryption is the process of converting cipher text into plain text.

FEATURES OF CRYPTOGRAPHY ARE AS FOLLOWS:

1. **Confidentiality:** Information is restricted to the intended recipient and cannot be accessed by others.
2. **Integrity**: Information cannot be manipulated during storage or transmission without being discovered.
3. **Non-repudiation**: The creator/sender cannot dispute sending information at a later date.
4. **Authentication** involves confirming the identities of both the sender and receiver. Additionally, the destination/origin of information has been validated.

TYPES OF CRYPTOGRAPHY:

In general, there are three forms of encryption:

1. **Symmetric Key Cryptography**: Messages are encrypted and decrypted using a single key shared by both the sender and recipient. Symmetric key systems are faster and simpler, but the sender and receiver must exchange keys securely. The most widely used symmetric key encryption technology is Data Encryption technology (DES).
2. **Hash Functions**: This algorithm does not need any keys. A fixed-length hash value is computed based on the plain text, making it difficult to reconstruct the plain text's contents. Many operating systems employ hash methods to encrypt passwords.
3. **Asymmetric Key Cryptography**: This approach uses a pair of keys for encryption and decryption.

STEGNOGRAPHY

Steganography is a technique for concealing communication by transforming a secret message into a phony one. Steganography is derived from Greek and meaning "covered writing". The fundamental principle underlying steganography is to avoid suspicion of the existence of the information.

FORMS OF STEGANOGRAPHY

Text: In this steganography, text can beutilized as a cover medium. To conceal the message, a word or line might be moved.

Whitespaces, as well as the amount and position of vowels, can be utilized to conceal a secret message. Audio stenography, which uses a digital representation of an audio recording, can conceal a secret message. It is simple to accomplish because a standard 16-bit file contains 216 sound levels, and a few levels variation would be undetect able to the human ear.

CONCLUSION

Cryptography is a means of preventing information and communications by using codes to safe guard our data from hackers. The material is intended to be read and processed. The prefix"crypt"denotes"hidden"or "vault," while the suffix "graphy" stands for "writing."Steg. Steganography is the process of concealing hidden information. Thus, steganography and cryptography techniques are extremely useful in protecting data from hackers.

References

1. Predictions and Trends for Information, Computer and Network Security[Online] available:http://www.sans.edu/research/securitylaborator y/article/2140.
2. A White Paper, Securing the IntelligentNetwork powered by Intel Corporation.
3. Network Security [Online] available: http://en.wikipedia.org/wiki/Network_security.
4. Network Security: History, Importance, and Future‖, University of Florida Department of Electrical and Computer Engineering, Bhavya Daya.
5. Ateeq Ahmad, ―Type of Security Threats and its Prevention", Ateeq Ahmad, Int.J.Computer Technology & Applications, Vol 3 (2), 750-752.
6. Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Incp. 257.
7. Dr. G. Padmavathi, Mrs. D. Shanmugapriya, A SurveyofAttacks,SecurityMechanismsand Challenges in Wireless Sensor Networks‖, (IJCSIS) International Journal of Computer ScienceandInformationSecurity,Vol.4,No.1 & 2, 2009.
8. Network Security Types of attacks [Online] available:http://computernetworkingnotes.com/network-securityaccess-lists-standards-and extended/types-of-attack.html.
9. Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia InternationalConferenceon,vol.,no.,pp.77-82, 13-15 May2008.
10. Securing the Intelligent Network [Online]available:http://www.trendmicro.co.in/cloudcontent/us/p dfs/security-intelligence/whitepapers/wp_idc_network-overwatchlayer_threatmngmt.
11. Hayatle O., Youssef A., Otrok H. Dempster-ShaferEvidenceCombiningforAnti-Honeypot Technologies.Inf.Sec.J.:AGlobalPerspective 21, 6 (January 2012), 2012, pp. 306-316. DOI: 10.1080/19393555.2012.738375.

******