JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Study on Enhancing LAN Using Cryptography and Other Modules

Dr. Prafullkumar Ashokrao Ghuge
Shankarlal Khandelwal Arts, Science & Commerce College, Akola

Abstract:

Enhancing the LAN with Cryptography and Other Modules" presents essential solutions to eliminate the inadequacies of the current network management systems. Remote machine control is made easier for the administrator with this powerful network feature.

There is a new suggested system called DSCSL that uses encryption, steganography, and LAN messaging (DSCSL) to ensure data security. When used together, these generally accepted methods aid in ensuring two-factor authentication (DFA). Companies, colleges, and other organisations can benefit from these security measures. Encrypting sensitive data in a scrambled form and hiding it behind a picture is a technique known as steganography.

At To the fullest extent possible, the network is put to use. It is proposed to use.net to implement the proposed system's functionality. There are a total of six modules in this product. A different aspect of the network is addressed by each of the modules. Monitoring, monitoring, remote processing and file transmission are only few of the features that may be found in the many modules. The following are the advantages that our system offers over the ones already on the market.

- The use of cryptography ensures the security of data during transmission via a network of interconnected nodes.

- Why use the Internet when we may use the high-speed Local Area Network (LAN) that already exists in practically all businesses and institutions?

• The broadcasting capability is 100 times faster than a peon distributing alerts to all employees, ensuring that messages are delivered on time and without error. Networks are becoming used for more than simply data exchanges. Data transfer may be put to good use in a variety of ways that are both entertaining and useful.

Time synchronisation is used in this case to allow the administrator to shut down a user system using a GPS receiver.

Keywords:

Lan, Cryptography, Modules, Network, Wake on LAN, Magic Packet.

Introduction:

In addition to moving from one computer to another, computer data is also encrypted as it travels. When the data is out of control, the data can be manipulated or faked for the advantage of persons with bad intentions. Using cryptography, our data may be transformed and restructured such that it is more secure when it moves between computers. In order to safeguard our data, the system is based on complex secret codes that utilise contemporary mathematics.

- Computer Security - a term used to describe software designed to prevent data breaches and other security breaches. Safeguarding your data when it is being sent via a network Security measures for the Internet's infrastructure
- Internet Security - Interconnected data collecting safeguards personal information

Viruses, Trojans, and other threats The person in charge of an organization's security requirements must have a systemic way to identify and define ways to meeting those criteria in order to evaluate their safety effectively. One method is to think about information security in terms of three dimensions:

- Security attack – Any actions that have an influence on the security of an organization's information.
- Security mechanism – A technique for detecting, preventing, or recovering from a security breach.

- Security service – A service that enhances the safety of the data management infrastructure and the transfer of firm information. One or more security measures are employed by the services to combat potential security issues.

Basic Concepts

- **Cryptography**

  The art or science of creating an unintelligible message via the use of ideas and methodologies.
- **Plaintext**

  In the beginning, there was a clear message.
- **Cipher text**

  The revised text Transpose and/or substitute the comprehensible message into an unintelligible one using a cypher algorithm.
- **Key**

  Information that only the sender knows about.

  Encrypt (encode) Using a key and cypher to encrypt plaintext
- Convert encrypted text to plaintext using a chip and key, decoding the process.

Cryptanalysis The study of concepts and methods for changing a message that does not include the key into a message that is comprehensible again. Sometimes referred to as "cracking code," The study of cryptography and the crystallisation of cryptology

Code Converting an understandable message into an encoded one.

Cryptography

Generally speaking, cryptographic systems may be categorised into three distinct subcategories:

Type of operations used for transforming plain text to cipher text

All the encryption algorithms are based on two general principles: **substitution**, in which each element in the plaintext is mapped into another element, and **transposition**, in whichelements in the plaintext are rearranged.

The number of keys used

If the sender and receiver uses same key then it is said to be **symmetric key (or) single key (or) conventional encryption**.

If the sender and receiver use different keys then it is said to be **public key encryption**.

The way in which the plain text is processed

- A **block cipher** processes the input and block of elements at a time, producing output block for each input block.
- A **stream cipher** processes the input elements continuously, producing output element one at a time, as it goes along.

Cryptographic Attacks

Passive Attacks

Eavesdropping and monitoring are essential in passive assaults because of the nature of the attack. The opposing party's purpose is to get the provided information. Passive assaults fall into two categories:

Content of the Message: A phone call, an email, or a file transfer containing sensitive or secret information are all examples of this. Our goal is to prevent a third party from reading the contents of any such conversations.

Traffic analysis: Even if we had encryption in place, the adversary might still decipher the message's pattern. The adversary can track the host's location and monitor the frequency of communications sent. This information might be important in determining the correspondence's value. Detection of passive assaults is extremely difficult due to the fact that no data is altered. However, it is possible to minimize the damage that these strikes do.

Active attacks

This may be done by altering the data source or creating an incorrect source. There are four distinct types of attacks:

- **Masquerade –** According to one witness, it's the work of a different witness. In order to have an unauthorized effect, a data unit is passively captured and subsequently sent. It is possible to change messages in order to generate an unapproved consequence, or to postpone and register a message.
- **Service denial –** Stops or slows down the usual usage of communication services. By disabling or overloading the network for output losses, a whole network can be interrupted to refuse service. There is no method to prevent active assaults since it would necessitate the physical security of all contact facilities and channels. Instead, the focus should be on anticipating such problems before they arise so that action may be taken to remedy any resulting delays or interruptions.

Major types of attacks

Network communication may be used to launch a wide variety of assaults. Attacks can take a variety of forms, including the following:

a) Risks to security:- Among the many hazards to a user's device are those that might result in the loss of sensitive data. Service denial, virus assault, spyware and Trojan horse are among the behaviors that fall under this umbrella of "malware". Intruding into databases and gaining unauthorised access to the Internet are also part of the activities.

b) Data capture and cryptanalysis:- During the transmission of data via a communications network, this assault is carried out. Retrieving the original data by copying or thieving sensitive data from networks.

c) Unauthorized installation of the applications:- Viruses and security holes can be introduced into a device by installing programs that are not approved or verified. In order to avoid this, only approved apps should be allowed, and unwanted programs such as audios, movies, games, or other online applications should be avoided entirely.

d) Unauthorized access:- Any unauthorised access to network resources or records might result in the loss of critical information. As a result, only precise methods of user identity authentication should be employed, and resource management should only be performed on occasion.

e) Virus Infection:- It is possible to lose or modify sensitive data when a virus, malware, Trojan horse, or spyware is employed for network or resource use Many network resources and components are destroyed when the source codes or hardware are created.

Research Methodology:

Based on the notion of distorting the message and concealing its existence, the design for the combination of two separate approaches is based on the idea of reversal of distortion and recovering the original message. Three modules are used in this design:

Cryptography Module

1. In this science, information is encoded into a form that cannot be deciphered.
2. Securely storing and transmitting sensitive data is made possible through the use of cryptographic techniques.

Steganography Module

1. It is possible to hide a secret message inside other messages with the help of the Steganography module.
2. Secret messages may be hidden in Graphic Images with this tool.

LAN Messaging Module

1. Typed text-based communication between two or more persons is called LAN Messenger (LM). Computers connected to a network transmit the text.
2. It's possible that LAN messaging is closer to actual discussion than e-"letter" mail's style since it allows for real-time communication and simple cooperation.

Wakeon LAN

A specific network communication known as a "magic packet" is used to implement Wake on LAN. The MAC address of the target machine is contained in the magic packet. Upon receiving a magic packet targeted to it, the listening computer begins system wake up. If you're utilizing the OSI model, you'll be sending the magic packet via the network broadcast address, not the IP address, to all NICs.

As a result, Wake on LAN may be used on any device. You can wake up machines on any platform with any program. When it comes to Wake on LAN, many people believe that it can only be utilized within the current network subnet. While this is usually the case, there are rare situations in which certain components of the network interface must remain on in order for wake on LAN to operate. Stabilizing power consumption is significantly lower than usual operational power consumption for this device.

Disabling wake-on-LAN when the machine is off but still plugged in may cut power usage marginally. Administrators can reactivate a system that has been shut down by a user using this module. Other machines on the network can be awakened with WakeOn Lan.

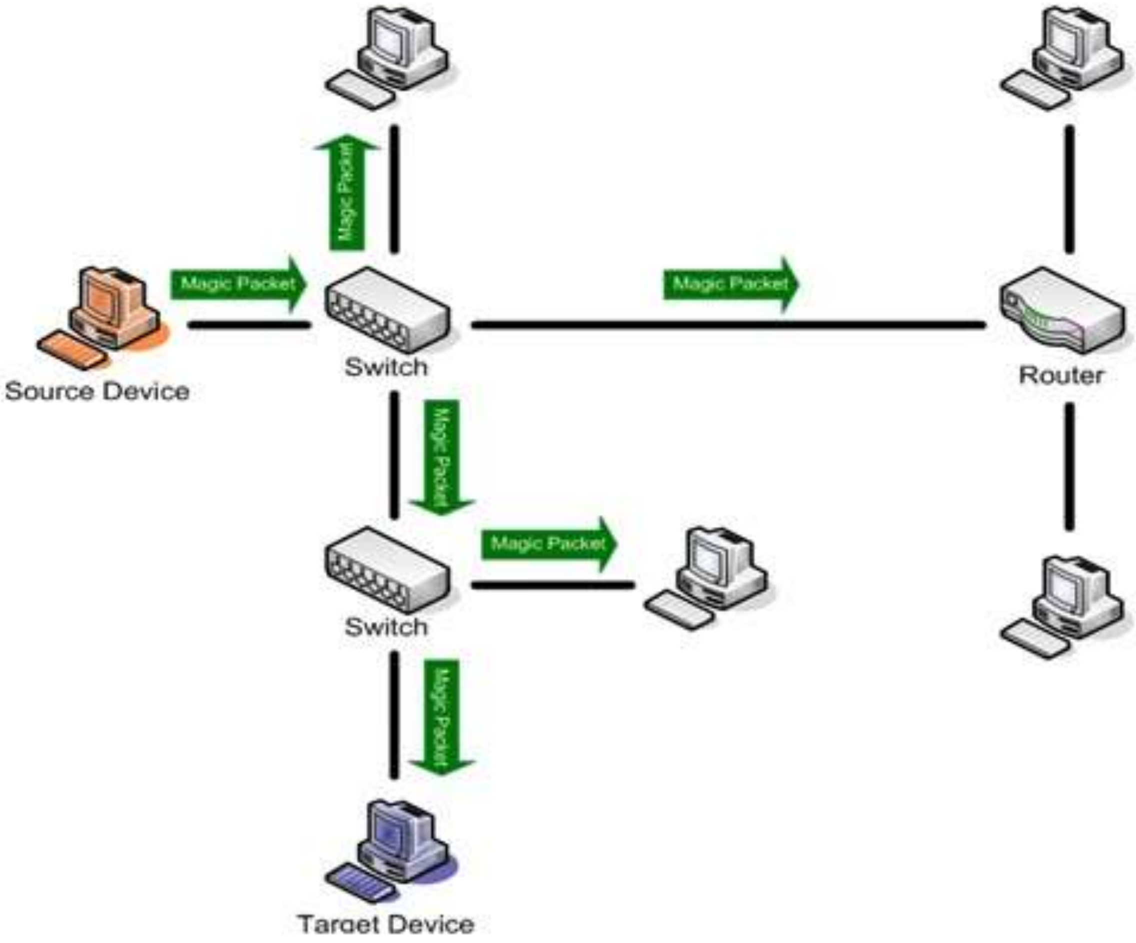

Figure 1: Wake on LAN

Magic Packet:

The magic packet is a broadcast frame that contains 6 bytes of all 255 (hexadecimal FF FF FF FF FF FF), followed by 16 repeats of the destination computer's 48-bit MAC address, wherever in its payload. Typically, the magic packet is delivered as a UDP datagram to port 7 or 9 or directly over Ethernet, but it may also be sent as any other network or transport layer protocol, as long as the string above is scanned.

The following are the basic constraints of a typical magic packet:

- Requires destination computer MAC address(also may require a Secure On password)
- Does not provide a delivery confirmation
- May not work outside of the local network
- Requires hardware support of wake on LAN on destination computer

In order to minimize power consumption, the wake on LAN implementation is designed to be relatively basic and to be swiftly processed by the circuitry present on the Network Interface Card (NIC). Wake on LAN requires a MAC address since it acts underneath the protocol layer, rendering IP addresses and DNS names useless.

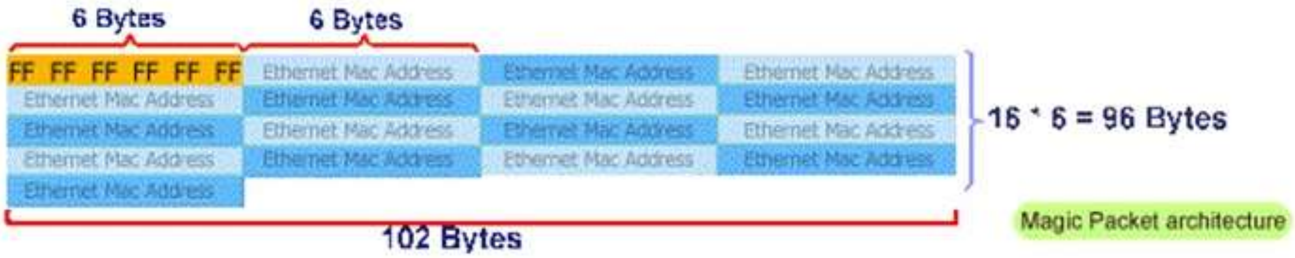

Figure 2: Magic Packet Architecture

Any action taken by a subordinate may be monitored and controlled by the administrator. Data and files can be protected by encrypting them. Even if the user system is turned off, the administrator can still administer it. In order to use the GPS time to synchronize the system time of computers connected to the network, we may use the satellite timing system and construct an application (client and server) for this purpose.

DSCSL offers a safe and convenient means to transport files and messages over networks while also protecting the data contained inside.

1. The DSCSL and its associated modules are used in a wide range of industries, including small-scale industrial environments, colleges and universities, and the military for security purposes.
2. Using DSCSL is a breeze because of the software's intuitive GUI (Graphical User Interface) forms.
3. In order to keep its data safe, the military constantly relies on this type of protection.
4. In the banking sector, this method may be used in any situation, such as transaction ID, bank statement, and account detail, among others.

Conclusion:

Since our system provides two levels of security for data, we conclude that it is a good fit for our needs. Now that LAN messenger and steganography have been combined for the first time, it will be advantageous for the transmission of all secret messages and information. Send files over the network in a safe manner.

Network-to-network data transmissions require the use of cryptography as a safeguard. To keep them safe, it used data against unauthorized users. Sender and recipient can more safely exchange the key. Techniques like encryption, watermarking, digital signatures, and firewalls can all be used to safeguard sensitive security data. We might presume that cryptography has shown to be a key to securing our sensitive information because of the increasing use of cryptographic technologies.

References:

1. www.ntp-time-server.com
2. www.edu-observatory.org/gps
3. https://en.wikipedia.org/wiki/Wake-on-LAN
4. https://www.codeproject.com/KB/IP/WOL.aspx
5. https://en.wikipedia.org/wiki/Data_Encryption_Standard
6. Cryptography and Network Security: Atul Kahate
7. Westfield A. and Pitman A. "Attacks on Steganography Systems". Lecture Notes in Computer Science, Springer-Velar, Berlin 2000, pp. 61-75.
8. Cvejic N. Seppanen, T., “Increasing robustness of LSB audio steganography using a novel
9. Preneel, B. (2010, September). Cryptography for network security: failures, successes and challenges. In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (pp. 36-54). Springer, Berlin, Heidelberg.

10.Bhatia, P., & Sumbaly, R. (2014). Framework for wireless network security using quantum cryptography. arXiv preprint arXiv:1412.2495.

11.Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology, 10(5), 763- 770.

12.Stallings, W. (2006). Cryptography and Network Security, 4/E. Pearson Education India