ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Special Issue , August 2019

International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

Cryptography Network Security

V.Lakshmi, G.Sujatha, K.Anusha, B.Hari Priya

U.G. Student, Department of Computer Science Engineering, Sree Vahini Institute of Science & Technology

ABSTRACT: The rapid development of computer network system brings both a great convenience and new security threats for users. Network security problem generally includes network system security and data security. Specifically, it refers to the reliability of network system, confidentiality, integrity and availability of data information in the system. Network security problem exists through all the layers of the computer network, and the network security objective is to maintain the confidentiality, authenticity, integrity, dependability, availability and audit-ability of the network. This paper introduces the network security technologies mainly in detail, including authentication, data encryption technology, firewall technology, intrusion detection system (IDS), antivirus technology and virtual private network (VPN). Network security problem is related to every network user, so we should put a high value upon network security, try to prevent hostile attacks and ensure the network security

KEY WORDS: Encryption, Decryption, Cryptography , Network Security,Computer Networks.

I. INTRODUCTION

Network security 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 security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Computer security, **cybersecurity**[1] or **information technology security** (**IT security**) is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. The field is becoming more important due to increased reliance on computer systems, the Internet[2] and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smart phones, televisions, and the various devices that constitute the "Internet of things". Due to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.[3]

II. SIGNIFICANCE OF THE SYSTEM

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Within the context of any application-to-application communication, there are some specific security requirements, including:

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Special Issue , August 2019
International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

III. LITERATURE SURVEY

- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message. There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use.
- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption Secret key cryptography algorithms that are in use today include: Data Encryption Standard (DES): The most common SKC scheme used today, DES was designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS) [now the National Institute for Standards and Technology (NIST)] in 1977 for commercial and unclassified government applications. DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks. IBM also proposed a 112-bit key for DES, which was rejected at the time by the government; the use of 112-bit keys was considered in the 1990s, however, conversion was never seriously considered. The DEA, often called DES, has been extensively studied since its publication and is the best known and widely used symmetric algorithm in the world. Advanced Encryption Standard (AES): In 1997, NIST initiated a very public, 4-1/2 year process to develop a new secure cryptosystem for U.S. government applications. The result, the Advanced Encryption Standard, became the official successor to DES in December 2001. AES uses an SKC scheme called Rijndael, a block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen. FIPS PUB 197 describes a 128-bit block cipher employing a 128-, 192-, or CAST-128/256: CAST128, described in Request for Comments (RFC) 2144, is a DES-like substitution-permutation crypto algorithm, employing a 128-bit key operating on a 64-bit block. CAST-256 (RFC 2612) is an extension of CAST-128, using a 128-bit block size and a variable length (128, 160, 192, 224, or 256 bit) key. CAST is named for its developers, Carlisle Adams and Stafford Tavares and is available internationally. CAST-256 was one of the Round 1 algorithms in the AES process 256-bit key. (iii) INTRUSION DETECTION It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic.

We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called Intrusion Detection. The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The recent denial of service attacks on major Internet sites have shown us, no open computer network is immune from intrusions. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of deferenc. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. Many intrusion detection techniques have been developed on fixed wired networks but have been turned to be inapplicable in this new environment. We need to search for new architecture and mechanisms to protect wireless networks and mobile computing application. We examine the vulnerabilities of wireless networks and say that we must include intrusion detection in the security architecture for mobile computing environment. We have showed such architecture and evaluated key mechanisms in this architecture such as applying mobile agents to intrusion detection, anomaly detection and misuse detection for mobile ad-hoc networks.

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Within the context of any application-to-application communication, there are some specific security requirements, including:
 Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)

It is very important that the security mechanisms of a system are designed so as to *prevent* unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of

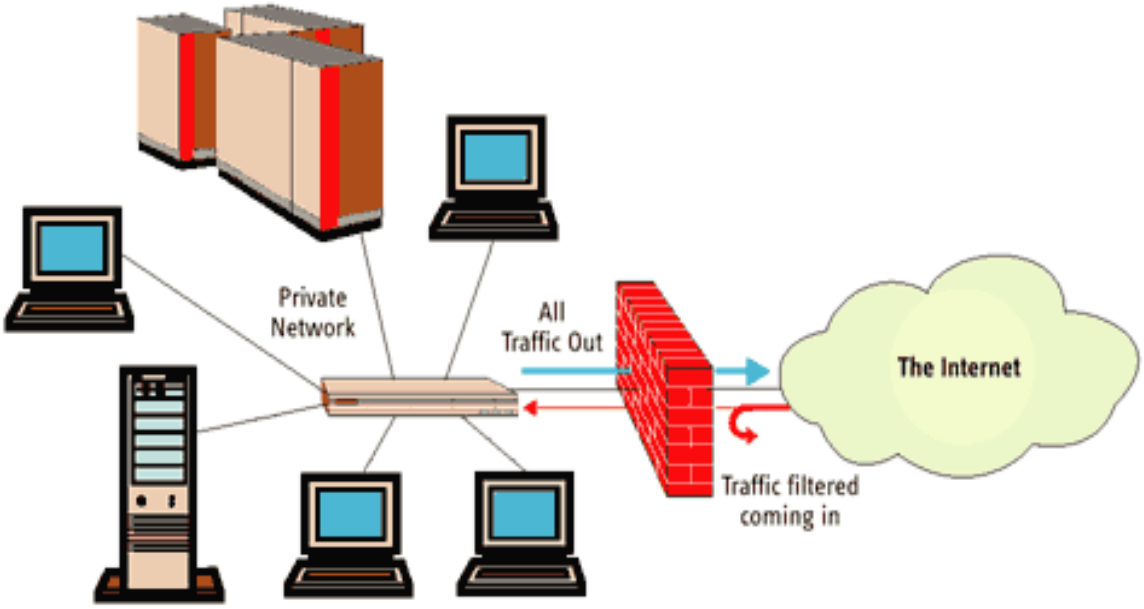
ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Special Issue , August 2019
International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

research is called Intrusion Detection. A simple firewall can no longer provide enough security as in the past. Today's corporations are drafting intricate security policies whose enforcement requires the use of multiple systems, both proactive and reactive (and often multi-layered and highly redundant). The premise behind intrusion detection systems is simple: Deploy a set of agents to inspect network traffic and look for the ―signatures‖ of known network attacks. However, the evolution of network computing and the awesome availability of the Internet have complicated this concept somewhat. With the advent of Distributed Denial of Service (DDOS) attacks, which are often launched from hundreds of separate sources, the traffic source no longer provides reliable temporal clues that an attack is in progress. Worse yet, the task of responding to such attacks is further complicated by the diversity of the source systems, and especially by the geographically distributed nature of most attacks. Intrusion detection techniques while often regarded as grossly experimental, the field of intrusion detection has matured a great deal to the point where it has secured a space in the network defense landscape alongside firewalls and virus protection systems. While the actual implementations tend to be fairly complex, and often proprietary, the concept behind intrusion detection is a surprisingly simple one: Inspect all network activity (both inbound and outbound) and identify suspicious patterns that could be evidence of a network or system attack**.**

IV. METHODOLOGY

A.FIREWALLS

A firewall is a system that enforces an access control policy between two networks—such as your private LAN and the unsafe, public Internet. The firewall determines which inside services can be accessed from the outside, and vice versa. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one to block traffic, and one to permit traffic. A firewall is more than the locked front door to your network—you're your security guard as well. Different types of Firewalls: 1. Packet



B. CRYPTOGRAPHY :(DES Vs AES)

Does increased security provide comfort to paranoid people? Or does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Special Issue , August 2019

International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient. The search for a replacement to DES started in January 1997 when NIST announced that it was looking for an Advanced Encryption Standard (AES).

C.NEED FOR INTRUSION DETECTION

A computer system should provide confidentiality, integrity and assurance against denial of service. However, due to increased connectivity (especially on the Internet), and the vast spectrum of financial possibilities that are opening up, more and more systems are subject to attack by intruders. These subversion attempts try to exploit flaws in the operating system as well as in application programs and have resulted in spectacular incidents like the Internet Worm incident of 1988. There are two ways to handle subversion attempts. One way is to prevent subversion itself by building a completely secure system. We could, for example, require all users to identify and authenticate themselves; we could protect data by various cryptographic methods and very tight access control mechanisms. However this is not really feasible because: (1) In practice, it is not possible to build a completely secure system. Miller gives a compelling report on bugs in popular programs and operating systems that seems to indicate that (a) bug free software is still a dream and (b) no-one seems to want to make the effort to try to develop such software. Apart from the fact that we do not seem to be getting our money's worth when we buy software, there are also security implications when our E-mail software, for example, can be attacked. Designing and implementing a totally secure system is thus an extremely difficult task. (2) The vast installed base of systems worldwide guarantees that any transition to a secure system, (if it is ever developed) will be long in coming. (3) Cryptographic methods have their own problems. Passwords can be cracked, users can lose their passwords, and entire crypto-systems can be broken. (4) Even a truly secure system is vulnerable to abuse by insiders who abuse their privileges. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013 217 (5) It has been seen that that the relationship between the level of access control and user efficiency is an inverse one, which means that the stricter the mechanisms, the lower the efficiency becomes. The history of security research has taught us a valuable lesson – no matter how many intrusion prevention measures are inserted in a network, there are always some weak links that one could exploit to break in.

VI. CONCLUSION AND FUTURE WORK

The diligent management of network security is essential to the operation of networks, regardless of whether they have segments or not. It is important to note that absolute security is an abstract concept – it does not exist anywhere. All networks are vulnerable to insider or outsider attacks

REFERENCES

1. Cryptography and Network Security by William Stallings-2nd Edition
2. Network Security Fundamentals by Gert Delaet, Gert Svhauwers
3. Cryptography and Network Security by Kahate
4. Cryptography and Network Security by P S Gill.
5. Cryptography and Network security by William Stallings-5th editio