Network Security and Cryptography

Ms. Tejashri Maruti Dumbre
HOD of Department Information Technology
tejashridumbre89@gmail.com

Ms. Swati Dadabhau Jaid
Information Technology
Jaidswati123@gmail.com,

Ms Priyanka Dnyaneshwar Dherange
Information Technology
priyadherange30@gmail.com

ABSTRACT

Now security has become a serious and sensible issue either it may be in "Real World" or in the "Cyber World".in this world as against to the cyber world an attack is often started by information gathering.

Network security is a complicated subject,ancient only tackled by well-trained and experienced experts.however,as more and more people become "wired",an increasing number people need to understand the basics security in a networked world.

The main aim of this paper is to provide a broad review of network security and cryptography,with particular consider to digital signatures.Network security and cryptography is a subject too broad ranging to coverage about how to protect information in digital form and to provide security services.

The security mechanisms are mainly based on cryptographic algorithms like symmetric-DES,AES,asymmetric-RSA,ECC.The logical conclusion is to use both kind of algorithms and their combination to achieve optimal seed and security level.

Index Terms-Network security,hash function ,MAC algorithm,cryptographic algorithm,block cipher,stream cipher

1. INTRODUCTION

The world is becoming more interconnected with internet and new networking technology such as cryptography,stegnography,etc.A network security has become more important to personal computer users,organization,military,and government. Network security is nothing but any protection of access,misuse and hacking of files or directories in computer network system.There are most common threats to a network such as viruses,worms,spyware and adware and identity theft .By inceasing network security , decrease the chance of privacy spoofing,identity or information theft and so on.

A network security capture a different types of computer network, both private and public ,that are used in real time jobs; conducting transaction and communication among business,government agencies and individuals.Cryptography is an important factor in network security.Using cryptography we can give security to any file,document or directories.Cryptography is a science that uses a complex mathematics and logic to design a strong encryption method.The most common earlier way of protecting a network resources is by give it a unique identity corresponding to the password.

2. HISTORY

Recent interest in security was fueled by the crime commited by kevin Mitnick .Kevin Mitnick commited the largest computer related crime in U.S. history. The losses were eighty million dolars in U.S. intellectual property and source code from a different types of companies.Since then information security came into the spot light .Public networks are being relied upon to deliver financial and personal information .Due to the estimation of information that is made accessible through the internet.information security is required to evolve.Due to Kevin Mitnick soffense ,companies are emphasizing security for the intellectual property.Internet has been a driving force for data security improvement.Before the modern era,cryptography was concerened solely with message confidentiality conversion of message from a understandable form into an unintelligible one and back again at the other end,rendering it unreadable by interceptors or eavesdroppers without secret knowledge.Encryption attempted to ensure secrecy in communications

3. WHAT IS NETWOK SECURITY

Network security is the security provide to network from unauthorized access and risks.It is the duty of network administrators to adopt preventive measure to protect their networks from potential security threats.Computer network that are involved in regular transactions and communications with in the government,individuals,business requires security.The simple way of protecting a network resource is by assigning it a unique name and corresponding password .
Network security consist of the policies and practices adopt to prevent monitor unauthorized access ,misuse,modification,or denial of computer network and network accessible resources .Network security involve the authorization of access to data in a network,which is control by the network administrator

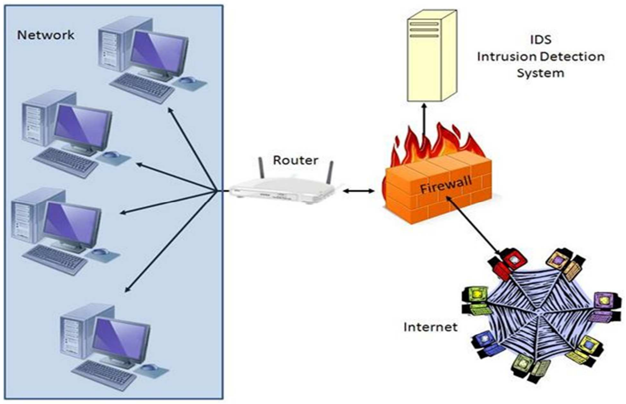

Fig 3.1 Network Security

3.1.1. TYPES OF NETWORK SECURITY

- Distributed Denial of Service(DDoS)Prevention
- Firewall
- Intrusion prevention or detection system(IPS/IDS)
- Security information and event management(SIEM)
- Network Access Control(NAC)
- Virtual Private Network(VPN)
- Secure Network Equipment
- Data Loss Prevension(DLP)
- Web Content Filter
- Anti-Malware
- Access Control

1) **Distributed Denial of Services(DDoS)prevention:**
A Distributed Denial of Services(DDoS) attack is an attack in which multiple compromised system attack a target,such as a server,website or alternate network facility,and cause a denial of service or users of the selected resource .The flood of incoming message,connection request or malformed packets to the target system forces it to slow down or even dash and shutdown,thereby denying service to authorized users or system

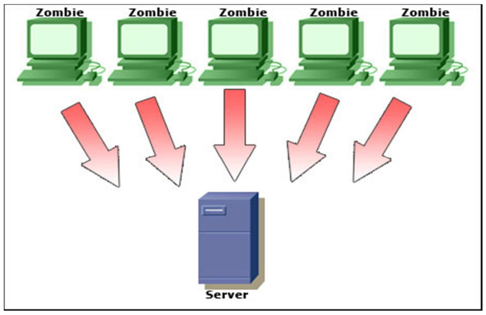

Fig.DDoS attack

Firewall:
A firewall is a network security system that check and manage the incoming and outgoing network traffic based on preset security rules.A firewall typically establishes a hurdle between a trusted,protected internal network and another outside network,such as the internet,that is assumed not to be secure or trusted.
Types of firewall:
1.Network layer or packet filters
2.Application layer

3.Proxies
4.Network address translation

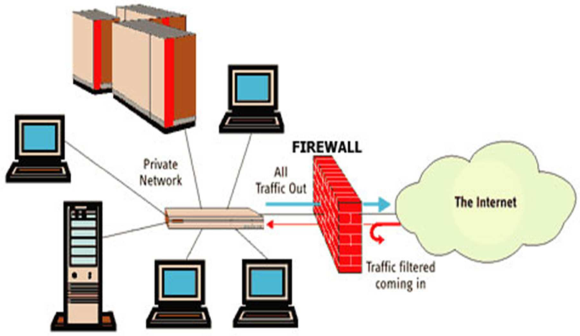

Fig Firewall

TYPES OF COMPUTER SECURITY THREATS AND RISKS

1.Trojen:

Trojen is one of the most complex threats among all.Most of the popular banking threats come from the Trojen family such as Zeus and SpyEye.It has the ability to hide itself from antivirus detection and steal important banking data to compromise your bank account .If the Trojen is really powerful ,it can take over your entire security system as well .As a result, a trojen can cause many types of damage

money over destruction. As a result, Virus is only present for people who want to access it for some sort of revenge purpose starting from your own computer to your online account.

2. Virus. Looking at the technology 10 years back, Virus is something is very popular. It is a harmful program where it replicates itself and aim to only destroy a computer. The eventual goal of a virus is to ensure that the victim’s computer will never be able to operate properly or even at all. It is unpopular today because Malware today is designed to earn

Cryptography is the practice and study of capability for safe communication in the presence of third parties called adversaries.Cryptography is a method of storing and transmitting data in a particular form

WHAT IS CRYPTOGRAPHY

so that only those for for whom it is intended can read and process it.Cryptography prior to the modern was effectively similar with encryption,the conversion of information from a understandable state to clear nonsense. The creator of an encrypted message (Alice) shared the decoding technique needed to recover the original information only with intended recipients (Bob), thereby prevent unwanted persons (Eve) from doing the same. The cryptography information often uses Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve for the challenger. Since the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Classification of Cryptography

1.Symmetric Key Cryptography (Secret Key Cryptography)
2.Asymmetric Key Cryptography (Public Key Cryptography)

3.HashFunction

1.Symmetric Key Cryptography:

Symmetric-key algorithms are formula for cryptography that utiliza the similar cryptographic clue for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple modifiaction to go between the two keys.The keys, in practice, replace a shared secret between two or more parties that can be utilize to control a private information link. This requirement that both parties have entry to the secret key is one of the main disadvantage of symmetric key.

Types of symmetric-key algorithm:

1.Stream cipher

2.Block cipher:

1) **stream cipher:**

A **stream cipher** is a symmetric key code where plaintext digits are fuse with a pseudorandom cipher digit series .In a stream cipher, each plaintext digit is encrypted one at a time with the equivalent digit of the keystream, to give a digit of the ciphertext stream. Since encoding of each digit is dependent on the current condition of the cipher, it is also known as ***state cipher***. In practice, a digit is typically a bit and

The merging perform and exclusive –or

2)**Block cipher:**

In cryptography, a **block cipher** is a deterministic algorithm handle on fixed-length category of bits, called *blocks*, with an unvarying change that is specified by a symmetric key. Block ciphers operate as important elementary components in the sketch of many cryptographic protocols, and are widely used to execute encryption of bulk data.

CONCLUSION:

As we toward a society where automated information facility are increased and cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily access by using Cryptography technique. DES is now considered to be insecure for some applications like banking system. there are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable. By adding additional key, modified S-Box design, modifies function implementation and replacing the old XOR by a new operation as proposed by this thesis to give more robustness to DES algorithm and make it stronger against any kind of intruding. DES Encryption with two keys instead of one key already will increase the efficiency of cryptography.

ACKNOWLEDGEMENT:

First and foremost, we would like to thank my author Ms.DUMBRE.T.M.Ms.Jaid.Swati.D,Ms.Dherange priyanka.D. for his guidance and support. We will forever remain grateful for the constant support and guidance extended by guide, in making this paper. Through our many discussions and ideas. The led to the development of this paper.

REFERENCES:

- http://ieeexplore.ieee.org/document/6524439/
- http://www.engpaper.com/network-security-research-paper-12.html
- https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&cad=rja
- https://en.wikipedia.org/wiki/Cryptography
- http://www.interhack.net/pubs/network-security/
https://en.wikipedia.org/wiki/Network_security
- http://www.networkmonitoring.org/network-security-threats/