A Study on Network Security & Cryptography

Prof. Karishma Tiwari and Priya R.Verma
Asst. Professor and Research Scholar
St. Rock's College of Commerce and Science, Borivali (W), Mumbai, India

Abstract*:* *Network security is a Guarantee that all the devices in a network are working properly and the users of these devices only possess the rights /privileges that were granted to them.*
This can include:
Preventing unauthorized people from acting on the system maliciously preventing users from performing involuntary operations that are capable of harming the system. Securing data by anticipating failures making the Network and servers 100% available. These protocol required computer information to be confidential, available and have integrity.
Cryptography:-The process of converting a message into a secret code called CIPHER TEXT, and changing the encoded message back to regular text called PLAIN TEXT.
Encryption: The conversion of the original message into a secret code or CIPHER TEXT using a key.
Decryption:-The conversion of the encoded message or PLAIN TEXT back to the original message uses the same key.

Keywords: Network, Cryptography, Encryption, Decryption

I. INTRODUCTION

Network security consists of policies and practices adopted to prevent monitor from unauthorized access, misuse, modification, denial of a computer network and network accessible resources. It involves the authorization of access to data in a network, which can be modified by the network administrator. There are three main aspects of the network security prevention, protection, and security. Ultimately, the overall goal of the network security is to create a connected network that protect against illegal activity while allowing you to perform activities you need to. An unsecure network refers to "FREE WIFI" which can easily be founded near coffee shops, malls etc. where you do not need any special login to use free WIFI, which means you and anyone can else use the Wi-Fi. There are basically 14 types of network security. 1. Firewalls 2. Email Security 3. Anti-virus and Anti- Malware software's 4. Network Segmentation 5. Access Control 6. Application Security 7. Behavioral analytics 8. Data loss prevention 9. Intrusion Prevention systems 10. Mobile device security 11. Security Information Cryptography deals with creating documents that can be shared secretly over public communication channels • Other terms closely associated – Cryptanalysis = code breaking – Cryptology • Kryptos (hidden or secret) and Logos (description) = secret speech / communication • combination of cryptography and cryptanalysis • Cryptography is a function of plaintext and a cryptographic key.

II. REVIEW OF LITERATURE

Security Attacks, Services and Mechanisms To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security: Security attack – Any action that compromises the security of information owned by an organization. Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack. Security service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

2.1 Objectives of the research

1. To Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.

2. To Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

III. RESEARCH METHODOLOGY

Secondary Data: It is based on the secondary data that is collected from books, the internet, etc. Research methodology refers to the systematic process and the various techniques, procedures, and tools used by researchers to conduct research, gather data, analyze information, and draw valid conclusions.

A Methodology for Network Security Design Figure I presents an outline of the methodology we have proposed. The following sections develop the ideas in detail. Specification Phase The idea of formalizing the distinction between the essence of a system (what it must do) and the implementation of the system (how it does what it must do) derives from work on soft- ware development methodologies [6]. The application of this idea to network security design ensures that a problem- centered approach is taken and that the problem is fully under- stood before any implementation thinking occurs. We have found it useful to divide consideration of system specification into two components: statement of requirements and identification of constraints. Requirements are factors de- termined by the problem itself.

Constraints are factors that de- rive more from the environment of the problem than from the problem itself. For example, given that the problem is to pre- vent disclosure of transmitted data, a requirement would be to transmit the data.

IV. FINDINGS

Vulnerabilities: Ongoing research continually identifies vulnerabilities in network protocols, software, and hardware. These vulnerabilities can be exploited by malicious actors.

Advanced Persistent Threats (APTs): APTs are a significant concern. These are long-term, targeted attacks by well-funded and highly skilled adversaries, often nation-states. Detecting and mitigating APTs is a complex challenge.

User Behavior: Human error remains a major cause of security breaches. Employees and users can unintentionally compromise network security through actions like clicking on phishing links.

IoT and BYOD: The proliferation of IoT devices and the Bring Your Own Device (BYOD) trend pose security risks as they introduce more entry points for attackers.

Regular Patching: Keep software and hardware up to date with security patches to address known vulnerabilities.

Intrusion Detection and Prevention: Implement robust intrusion detection and prevention systems to monitor network traffic for unusual activity.

User Training: Educate employees and users about cybersecurity best practices to reduce the risk of human errors and social engineering attacks.

Zero Trust Model: Adopt a Zero Trust security model, where trust is never assumed and verification is required from anyone trying to access network resources.

Network Segmentation: Segment your network to limit lateral movement for attackers. This helps contain breaches.

Security Information and Event Management (SIEM): Use SIEM tools to centralize the collection and analysis of security data, enabling better threat detection and response.

Quantum Computing Threat: The advent of quantum computing poses a potential threat to current cryptographic algorithms, as they can efficiently break widely used encryption methods.

Side-Channel Attacks: Attackers can exploit side-channel information like power consumption or electromagnetic emissions to break cryptographic systems.

Algorithm Weakness: Cryptographic algorithms can be found to have weaknesses over time, making them vulnerable to attacks.

V. SUGGESTIONS

Post-Quantum Cryptography: Invest in post-quantum cryptographic research to develop encryption methods that are resistant to quantum attacks.

Key Management: Implement strong key management practices to protect encryption keys from unauthorized access.

Regular Algorithm Review: Continuously assess and update cryptographic algorithms and protocols to address newly discovered vulnerabilities.

Multi-Factor Authentication: Use multi-factor authentication to add an extra layer of security beyond just cryptographic protection.

Open Standards: Prefer open and well-vetted cryptographic standards and avoid proprietary solutions to ensure transparency and scrutiny.

Secure Hardware: Use trusted hardware modules and secure enclaves to protect cryptographic operations from physical attacks.

Both network security and cryptography are dynamic fields that require ongoing research and adaptation to stay ahead of emerging threats. It's crucial for organizations to stay informed about the latest findings and best practices to protect their digital assets.

VI. CONCLUSION

With the explosive growth in the Internet, network and data security have become an inevitable concern for any organization whose internal private network is connected to question over cloud. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. The various schemes which are used in cryptography for Network security purpose.

Encrypt message with strongly secure key which is known only by sending and recipient end, is a significant aspect to acquire robust security in cloud. The secure exchange of key between sender and receiver is an important task.

The key management helps to maintain confidentiality of secret information from unauthorized users. It can also check the integrity of the exchanged message to verify the authenticity. Network security covers the use of cryptographic algorithms in network protocols and network applications.This paper briefly introduces the concept of computer security, focuses on the threats of computer network security. In the future, work can be done on key distribution and management as well as optimal cryptography algorithm for data security over clouds.

REFERENCES

[1]. Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS),University of Washington.
[2]. Algorithms: http://www.cryptographyworld.com/algo.htm
[3]. Data_Communication_and_Networking_by_Behrouz.A.Foro uzan_4th.edition
[4]. Bellare,Mihir;Canetti,Ran;Krawczyk