Security in Internet web-systems

Chinmay Nandkishor Mathakari

University of Massachusetts Lowell

Department of Computer Science

Abstract: - Security and privacy in web system is the biggest concern nowadays. Individuals who use the Internet to purchase, buy, or sometimes connect require that their messages be private and confidential. In this paper, I will discuss the various aspects of Web and networking security and its flaws. In this paper, I will discuss the components of the Internet and networking security and its weaknesses. This paper also discusses key networking security strategies such as firewalls, credentials, encryption, authentication, and integrity, the architecture of a web application assault, as well as attack methodologies. As a result, different security protection approaches connected to high-speed Online safety and computer safety in the real world are being researched, such as DNS, One-Time Passwords, and network defense like a group. This paper also examined viral outbreaks in rising networks and their remarkable growth speeds.

Motivation: - Cyber-security is a way of protecting devices or websites from malicious sites, links, and attacks that are aimed to steal information, destroy devices, or money extortion. Implementing effective measures is a challenge since attackers are becoming more efficient. Different attacks like phishing, Ransomware, social engineering, and malware attacks are designed for a specific purpose. There are 3 ways of cybersecurity first one is network security secondly cloud security and third is physical security. The operating system and network architecture together are called network security. Network security can consist of firewalls, servers, hosts, wireless access points, etc.

Introduction: The inability of having absolute confidence in a computer system's dependability and confidence is a crucial reality in Internet security and web programs. The practice of protecting and preserving personal organizational information and assets that are shared on the Internet is known as web security. Some of the crucial issues that might have an impact on a variety of Web consumers are online safety. Consumers who utilize the Web to trade, purchase, and sometimes even chat need their communications to be trustworthy and secure. This is a constantly evolving field. Administrators and cyber safety experts generate and embrace a wide range of terminology to characterize possible threats to computers and networks. Trojans, viruses/malware, and worms are examples of the terminology used to describe genuine security threats. Joke programs and spyware/grayware are phrases being utilized to describe incidents that may or may not be dangerous but are frequently irritating and unwanted. Any research on trust in online apps demonstrates that most of them are insecure. For example, one study found that 80% of web applications had at least one serious security concern, while another found that 50% have a highly risky rating. To understand web security breaches, we need to understand weaknesses in web components.

Components in Network security and Weaknesses: -The user side is created using a coding language, as are the SQL statements. The Hypertext Transfer Protocol (HTTP), which connects the application and database sides, is employed. Additionally, the organizational processes, which is what makes each website unique.

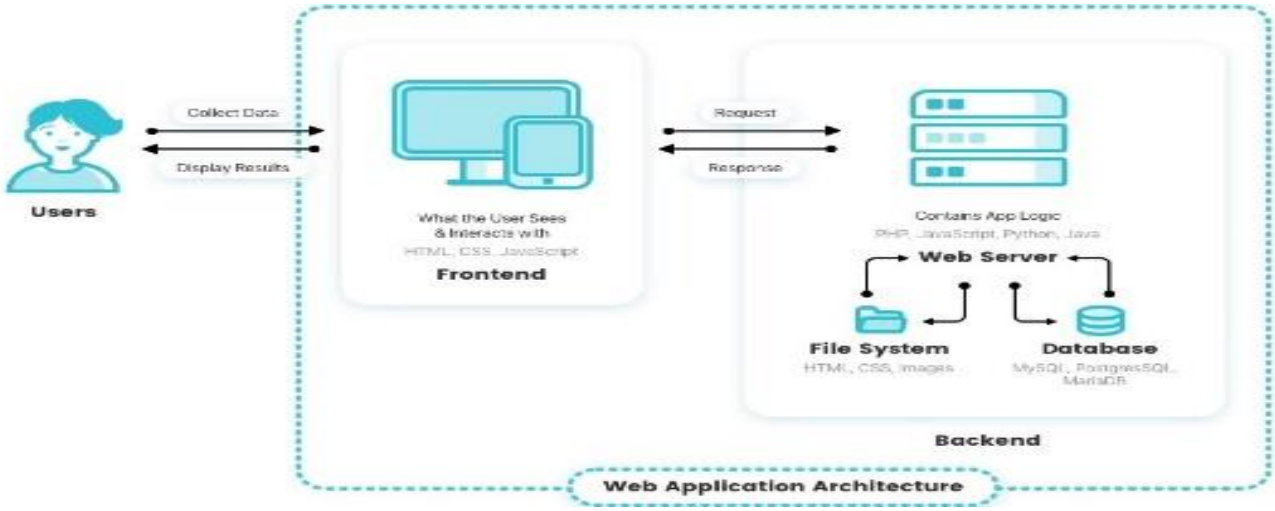

Fig 1. Components in web applications

Studies demonstrate that there are issues with administrative mistakes that result in security vulnerabilities that do not appear immediately apparent on websites. Many of these issues are also resolved in the short term, which leads to other issues developing. As a result, it is possible to evaluate the cost of information and disclose sensitive data. Additionally, such flaws harm an institution's image. Companies mostly reliable on ready procreation tools like firewalls or intrusion detection systems but do not monitor them regularly resulting in weak security. Technological individuals may not fully comprehend the connection between a business issue and cybersecurity. Many of the time security related tasks are requested from non-security expert people without giving them proper training and time to learn security. This occurred mostly since several businesses want speedy fixes to relaunch their portals or address program faults. To understand different key networking security strategies, we need to understand the attacker's approach to how a malicious person tries to attack the system.

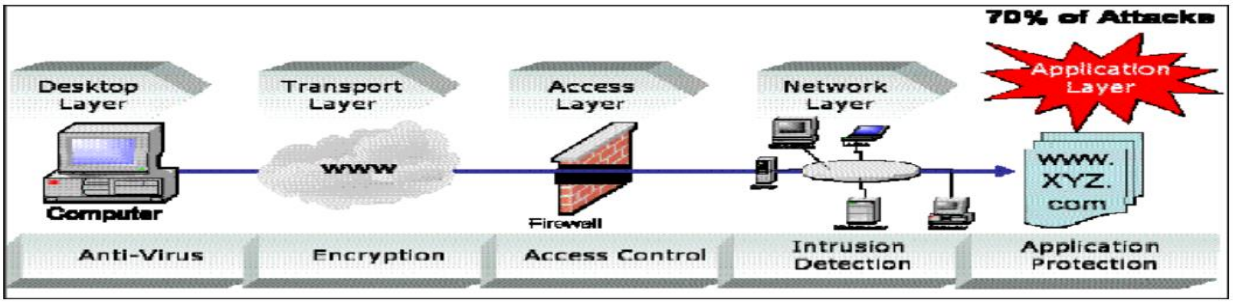

Fig. 2: attacker's approach

As shown in Fig 2 Attacker will log in to the system as a normal user and after reaching to application layer where he/she will start attacking the system, the attacker will pass some intrusion detection system like a firewall. Here we need to understand there are two types of attacker's customer attackers and normal attackers. Customer attackers will take advantage of the normal user to gather data and harm information on another side normal attackers will try to get more advantage to get extra information to steal data.

Key networking Strategies: -

1. **Encryption :-**The technique of turning knowledge and data into a code, particularly to restrict usage for unauthorized access. There are few encryptions mechanisms cryptography is one of them. There are two types of cryptography mechanisms symmetric key mechanisms and asymmetric key.

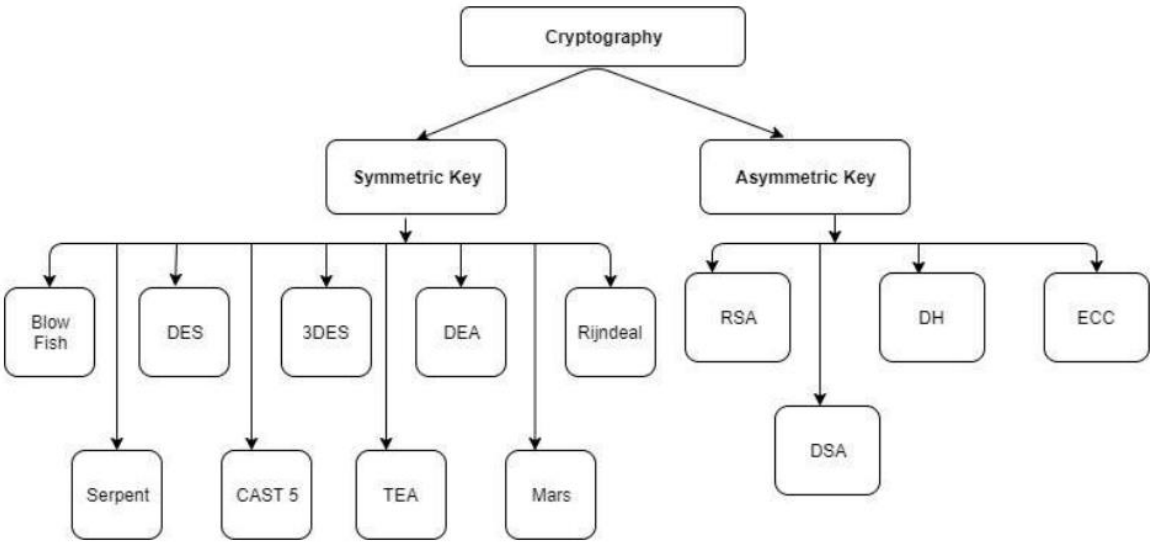

Fig 3 Symmetric and Asymmetric Encryption Method

In symmetric key cryptography, the same key is used between the sender and receiver for the encryption/decryption method (Delfs & Knebl, 2015).

symmetric key cryptography has different algorithms out of which DES, and 3DES were popular.

1. DES: - IBM created DES(Data Encryption Standard) in 1977 to safeguard information against unauthorized users. In DES Sender and the receiver use the same private key since it uses the same key for encoding and decoding a message. 16 round Feistel structures are used in the implementation of DES. DES uses key length of 56 bits.

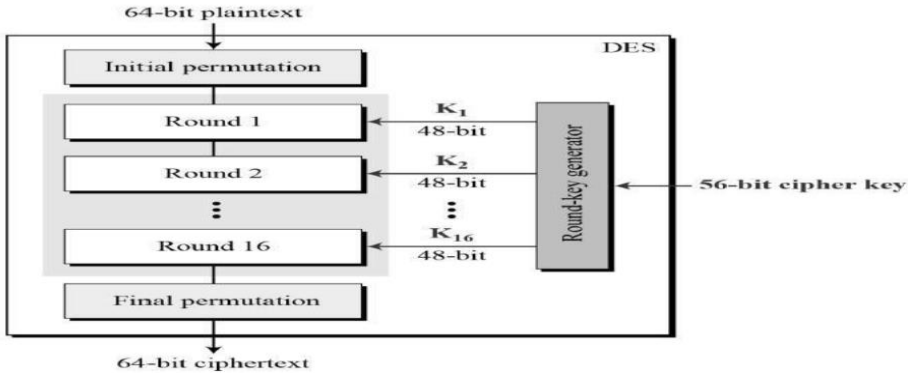

Figure 4: Working of DES

The most fundamental strategy for breaking any encryption is brute force, which is testing every key until you discover the one that works. The number of potential keys and, therefore, the viability of such an attack is determined by the key length. Finding the right key could take a total of 256, or around 72 quadrillion, attempts due to the effective DES key length of 56 bits. This is insufficient for DES data protection against computerized brute-force attacks. The short key length of DES led to the development of 3DES as a more secure substitute.

2. **3DES:** - The Data Encryption Standard (DES) cipher is used three times by the 3DES technique to encrypt data. Although 3des systems are certainly much slower than DES, but they are noticeably more secure than single DES.
3. **AES:** - Advanced encryption standard is Mostly used protocol now a days. It is because of higher length key sizes such as 128, 192, and 256 bits for encryption. Some benefits of using AES are
    1. more robust against hacking
    2. implemented in both hardware and software
    3. most common security protocol
    4. 2^{128} tries are required to overcome 128-bit encryption which makes it extremely hard to attack, making it a very safe protocol.

2. HTTPS or Secure Socket layer: - SSL Provides data exchange among a web browser and server security. All data exchanged between a web server and a browser is kept confidential and safe, which encrypts the connection between them.

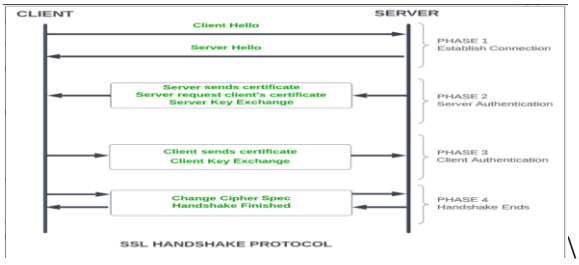

Figure 5. Working of SSL

Some benefits of using SSL include it is secure and reliable. The goal of SSL is to encrypt the information and made it available to only those who have access. Since information is sent over the internet there is a significant danger of falling into the wrong hands. SSL encrypts the data so that a third party cannot access data. This makes it ideal for securing data like User ID, payment methods, etc.

We occasionally receive spam phone calls or messages asking us to redirect to links, main purpose of such calls is to gather sensitive details like SSN, passport details, and credit card details. While visiting the link when a user does not notice the SSL certificate, they will not enter such websites. But at the same time Performance of the website which uses an SSL certificate, especially payment websites get drastically reduced. At the same time, we need to purchase an SSL certificate and set it up which is costly because of the maintenance involved, also SSL certificate needs to be renewed from time to time to ensure the validity of the certificate.

3. Firewall: - Firewalls operate in accordance with preset designs and guidelines. Track each data flow that passes through the firewall. Only approved data is permitted. Additionally logs the pertinent connection point, the server's communication presentation, and any intrusion attempts. To take control and tracing by administrators easier. A firewall can assist in preventing harmful malware from infecting your computer in addition to blocking undesired traffic. A firewalled system first performs a rule-based analysis of network traffic. Only incoming connections that a firewall has been set up to accept are welcomed. It achieves this by deciding whether to accept or reject a set of data packets—the units of communication you transmit across digital networks—in accordance with previously defined security criteria. A firewall acts as a traffic guard at the port, or entrance point, of your computer. Only reputable IP addresses or sources are permitted. In the same way that your postal address indicates where you reside, IP addresses are significant since they identify a machine or source. Hardware and software firewalls are also available. Each structure serves a unique yet important purpose. Like a router, a hardware firewall is situated physically between your networks and the gateway. A computer application that uses other programs and port numbers to function is known as an inner software firewall. In addition, there is a sort of cloud-based firewall called firewall as a service (FAAs). One benefit of cloud-based firewalls is that, like physical firewalls, they can grow with your company and provide efficient perimeter security. Firewalls may be categorized into several different groups according to how they are built and function. You can use any of the firewalls on the following list, depending on the size of your network and the level of security you want. Packet-filtering firewalls, Proxy service firewalls, Stateful multi-layer inspection (SMLI) firewalls, Unified threat management (UTM) firewalls, Next-generation firewalls (NGFW), Network address translation (NAT) firewalls, Virtual firewalls. There are some limitations of a firewall. Users may still visit dangerous websites; therefore, it cannot protect against internal threats or attacks. It also cannot stop the spread of virus-infected files or software. A firewall cannot shield you against password abuse or improperly implemented security policies. Firewalls are unable to defend against social engineering and other non-technical security concerns. Attackers using modems cannot be stopped or stopped by firewalls from calling into or out of the internal network. Firewalls are unable to protect compromised systems.

4. Intrusion Detection System: - Intrusion detection system is used to detect unexpected network activity and possible security exposures. The source of the intrusion, the location of the target, and the kind of potential penetration are then noted and recorded for fraudulent attacks. This information enables security professionals to quickly recognize and stop the assault before any damage has been done. Intrusion Detection System has been classified into different types some of them **are** Network intrusion detection systems (NIDS), Host-based intrusion detection systems (HIDS), Signature-based**, and** Anomaly-based. Limitations of IDS include it just assists in identifying attacks; it does not stop or hinder them. As a result, an IDS must be a component of an all-encompassing strategy that also includes other security measures and personnel who are trained to respond correctly. Also, it needs an experienced person to administer the IDS, also IDS do not process encrypted packets which makes them more vulnerable to attacks. we can read information from IP packets, but network addresses can be faked so attackers can use these addresses which makes it difficult to trace them.

Conclusion: - In this paper, I discussed some network security components and their limitations. It is also emphasized that using security prevention tools that we will explain later in this paper individually is not enough to secure a web application, these tools are like 1. Encryption and Decryption 2. HTTPS or Secure Socket layer, 3. Firewall, 4. Intrusion Detection System.

References: -

1.https://www.researchgate.net/publication/260793958_Survey_of_Web_Application_and_Internet_Securit y_Threats

2. https://docs.trendmicro.com/all/ent/imsec/v1.6/en-us/imsec_1.6_olh/About-Internet-sSecure.html#GUID-6E7DB3A0-B765-45A7-8DDF-3A45C31D07B7

3. https://www.ijrar.org/papers/IJRAR1ANP010.pdf

4. https://hal.archives-ouvertes.fr/hal-03024764/document

5. https://iopscience.iop.org/article/10.1088/1742-6596/1744/4/042037/pdf

6. https://www.rapid7.com/blog/post/2017/01/11/the-pros-cons-of-intrusion-detection-syste/#:~:text=An%20IDS%20cannot%20see%20into,until%20the%20intrusion%20is%20discovered.