IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 10, October 2020

DOI 10.17148/IJARCCE.2020.91026

Enhancing Network Security with Intrusion Prevention Systems and Host-Side Two-Factor Authentication

S.T.Saravanan[1], T.Manigandan[2], P.M.Suresh[3], Anbarasu.R[4]

Assistant Professor, Department of CSE, Bharathiyar Institute of Engineering for Women [1]

Assistant Professor, Department of CSE, SRS Engineering College and Technology, Salem, India [2]

Assistant Professor, Department of CSE, P.T.Lee Engineering College, Kanchipuram, India [3]

Assistant Professor, Department of CSE,P.T.Lee Engineering College,Kanchipuram,India[4]

Abstract: The foundational idea of overall network and computer security architecture is intrusion prevention. This technology holds significant value in both the corporate and academic domains. The Intrusion Prevention System (IPS) guards against misuse and unauthorized access, which is essentially an attack on computer and network resources, by keeping an eye on them. In this instance, we have applied two-factor authentication, which generates the one-time password on the host side rather than the server which makes it hard for anyone to enter. Additionally, it is recreated within a specific time frame without the assistance of outside sources. Thus, it's a simple method to go to our accounts.

Keyword: Intrusion Prevention System (IPS),computer security architecture.

I. INTRODUCTION

The number of computer systems and storage devices connected to the public network has greatly increased due to the explosion in Internet access and the widespread usage of broadband and mobile technologies. Due to our growing reliance on computer infrastructure, we discover that our intellectual property, private information, and vital IT assets are more vulnerable to cyber attacks than before. Network Intrusion Prevention Systems were created in response to the evolving threat landscape to offer more sophisticated protection than firewalls and intrusion detection systems alone. While intrusion prevention systems offer greater protection than firewalls and intrusion detection systems, they fall short in certain areas. Hussain [2] states that the procedure for stopping events from happening in a computer system or network.

II. RELATED WORKS

An intrusion prevention system (IPS) is a network security and threat prevention technology that audits network traffic flows to detect and stop vulnerability exploitation, according to Dr. S. Vijayarani in [10]. The terms "prevention system" refer to two different types: host (HIPS) and network (NIPS). In order to safeguard networks and systems, these technologies automatically monitor network traffic and take appropriate action. False positives and negatives are an IPS problem. An occurrence that triggers an IDS warning in the absence of an attack is known as a false positive.

A false negative is an occurrence that, in the event of an assault, does not trigger an alarm. Single points of failure, signature updates, and encrypted traffic are examples of bottlenecks that might result from inline operation. The activities taking on in a system or network is measured by IDS. Hussain states in [2] that there have been significant advancements made to IDS/IPS products. They're all still quitecomparable to their initial iteration, which began with a 1986 academic publication. Even with today's technology, next-generation intrusion prevention systems (NGIPSs), classic IDS/IPSs, andin firewalls of the next generation (NGFWs). Following Dorothy E. Denning's publication of "An Intrusion-Detection Model," Stanford Research Institute (SRI) created the Intrusion Detection Expert System (IDES). This paper served as the foundation for the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

The system employed statistical anomaly detection, user and host system profiles, and signatures to identify malicious network activities. Intrusion detection and prevention systems (IDS/IPS) are still evolving today and this trend is probably going to continue as threat actors adapt their methods and strategies for breaching networks. So far, we have examined how the IDS/IPS concept originated in an academic publication and evolved throughout time until 2005.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 10, October 2020
DOI 10.17148/IJARCCE.2020.91026

According to [9], it was investigated that in 2008, hackers were directing users to their website by means of frame redirects on well-known websites, such as news sites.

I frame code would drive users to a malicious website if they were on one of those well-known websites and their web browser or application had weaknesses. IDS/IPS providers were forced to respond by offering more countermeasures. Vendors provided information to block dangerous command and control IP addresses and websites that were known to host malware, in addition to pattern matching, string matching, anomaly detection, and heuristic-based detection. This decreased the time it takes to detect threats. Following the 2011 hack at RSA, a security firm well recognized for its two-factor authentication solution, another update to IDS/IPS was made. They started utilizing known-to-be-faulty files' MD5/SHA checksums. Each file's checksum is distinct. Checksums are character strings composed of numbers and letters that are used to confirm the integrity of files and text messages. They are also referred to as hashes or signatures.

The vendor's checksum on file and the one that entered the network would match, and the sandbox would notify the victim's business that malware had just entered the network. This was a significant development for network security back then. These days, NGFWs employ this kind of technology. To solve this problem, the cryptography key was created. In [11] the authors stated that The Cryptography is one of the most useful fields in the wireless communication area and personal communication systems, where information security has become more and more important area of interest. Cryptographic algorithms take care of specific information on security requirements such as data integrity, confidentiality and data origin authentication. A hash function generates a fixed-sized output message from an input message of variable size.

The result is commonly known as the message digest, hash code, or hash value. Hashing functions are important in today's cryptography applications. In computer cryptography, the Secure Hash Algorithm, or SHA, is a well-known message compression standard that may condense a lengthy message into a brief message abstract. In [11] SHA algorithm is classified and studied further as SHA-1 is a cryptographic hash function designed by National Security Agency (NSA) and published by National Institute of Standard and Technology (NIST) as a U.S Federal Information Processing Standard (FIPS).The four algorithms for secure hash functions are SHA-0, SHA-1, SHA-2, and SHA-3. SHA stands for Secure Hash Algorithm.SHA-1, which was initially developed in 1995 and is currently the most popular SHA hash function, is extremely similar to ordinary SHA-0 but fixes a mistake in the original SHA hash specification that caused a serious weakness.

These days, it is utilized in many different applications, such as TLS, SSL, SSH, and PGP. Within [12] A cryptographic hash function needs to be resilient against every kind of known cryptanalytic attack.It must, at the very least, possess the following characteristics of a secure cryptographic function: An arbitrary length message block can be applied to with the CHF H. 1. It generates a fixed-length output, h. 2.

The computation of h for a given M is not too difficult. 3. Pre-image Resistance: It is not possible to create M in such a way that H(M)=h given h. Fourth Preimage Resistance: Given a message M, it is difficult to find a second message M" such that H(M)=H(M"). 5. Collision Resistance: It is impossible to find H(M)=H(M") given M≠M". 6. Pseudo-randomness: The value h needs to be both random and deterministic with respect to its input.

The development of CHFs that meet these requirements has advanced significantly in recent years. A weak hash function (CHF) is one that satisfies the first five requirements listed above. One of the most basic hash functions [1, 57] combines a one-bit circular shift or rotation of the hash code for each block with bit-by-bit exclusive-OR (XOR) of the data for each message block. While this process offers a fair level of data integrity, it ideally falls short of offering sufficient collision protection when the encrypted hash value is used on a straightforward plaintext communication. The Message Digest (MD) family and the Secure Hash Algorithm (SHA) have been the most popular CHF. In this study, we mainly investigate the SHA family. The SHA family algorithms and the MD family algorithms share a similar structure.

III. METHODOLOGY

The Secure Hashing Algorithms (SHA) are a group of cryptographic operations that are intended to protect data. It functions by applying a hash function to modify the data. The cryptographic hash function known as SHA-1 (Secure Hash Algorithm 1) takes an input and outputs a 160-bit (20-byte) hash value called a message digest, which is usually represented as a 40-digit hexadecimal number. The National Security Agency of the United States created it, and it is a Federal Information Processing Standard.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 10, October 2020
DOI 10.17148/IJARCCE.2020.91026

Fig 1: Secure Hashing Algorithms (SHA)

In order to better protect user credentials and the resources they can access, two-factor authentication (2FA), also known as two-step verification or dual factor authentication is a security process in which the user provides two distinct authentication factors to verify themselves. Compared to authentication techniques that rely on single-factor authentication (SFA), where the user gives just one factor—typically a password or passcode—two-factor authentication offers a higher level of assurance. Users using two-factor authentication must supply both a password and a second factor, which is typically a security token or a biometric (such as a fingerprint or face scan).

The Secure Hash Algorithm (SHA) is used in two factor authentication (2FA) to generate a four-digit code that is time-dependent and changes every thirty seconds. The National Institute of Standards and Technology (NIST) released a series of cryptographic hash functions known as the Secure Hash Algorithms as a Federal Information Processing Standard (FIPS) for the United States.

The Secure Hash Algorithms (SHA) is a group of cryptographic functions that are intended to maintain the security of data. It functions by converting the data using a hash function, which is a method made up of compression functions, bitwise operations, and modular additions. After that, the hash function generates a fixed-size string that differs greatly from the original. Since these methods are one-way functions, it is nearly hard to change them back into the original data once they have been converted into their corresponding hash values. SHA-1, SHA-2, and SHA-3 are a few noteworthy algorithms that were developed with progressively stronger encryption in response to hacker attempts. For example, SHA-0 is no longer in use because of the extensively known weaknesses.

Since the server side only needs to maintain track of a particular user's hash value and not the actual password, SHA is frequently used to encrypt passwords. This is useful in the event that a database hacker gains access because they will only be able to decipher the hashed functions and not the real passwords. If the attacker tried to enter the hashed value as a password, the hash function would translate it into a different string and block access. SHAs also display the avalanche effect, in which a small change in the number of encrypted letters results in a large change in the output, or in the opposite, where highly diverse strings provide comparable hash values. Because of this consequence, hash values become useless in providing details about the input string, including its initial length. Furthermore, SHAs are employed in the detection of data manipulation by adversaries. In the event that a text file undergoes minor and imperceptible changes, the hash value of the modified file will differ from the original file's hash value, indicating a significant degree of tampering.

IV. OVERVIEW OF TOTP

In an early days of the Internet, when remote access was uncommon and there was just one attack type, this kind of authentication proved to be effective. These days, Trojans can overcome password security technologies by recording the user's keyboard strokes and even decrypting the user's login credentials and password by gathering the mouse click locations. The proposal was made to implement Two-Factor Authentication (2FA) in order to improve security. Two-factor authentication (2FA) verifies a user's claimed identity by combining two distinct factors: 1) something they possess, 2) something they know, or 3) something they are; for example, a password combined with tangible objects like smart cards, cell phones, tokens, or fingerprints. However, when a physical entity is employed as the second authentication factor—where numerous more operation steps are added—two-factor authentication causes discomfort to consumers as compared to password-based single-factor authentication.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 10, October 2020
DOI 10.17148/IJARCCE.2020.91026

For instance, the dynamic token approach offers great security and only requires a one-time password, but it necessitates carrying different tokens each time a user visits a different website. Jiliang [4] claims that second factor authentication eliminates the need for the user to engage with the device in a laborious way because it is totally visible to the user. As a result, our suggested T2FA demonstrates anti-fraud capabilities and has promising application prospects.

The Secure Hashing Algorithms (SHA) are a group of cryptographic operations that are intended to maintain the security of data. It functions by applying a hash function to modify the data. The 160-bit (20-byte) hash value known as a message digest is produced by the cryptographic hash function SHA-1 (Secure Hash Algorithm 1) from an input. This value is usually displayed as a 40-digit hexadecimal number. It is a U.S. Federal Information Processing Standard that was created by the National Security Agency.

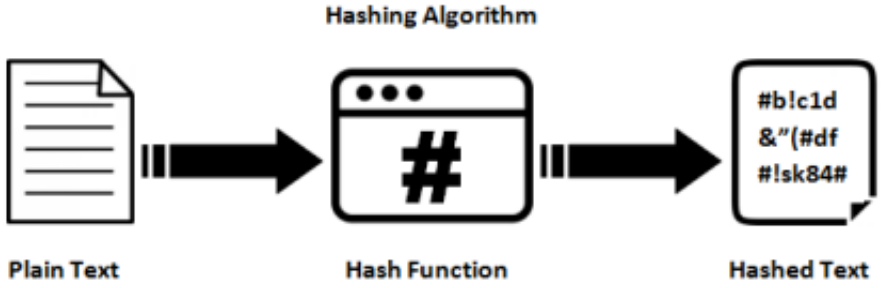

Fig 2 : Hashing algorithm

V. CONCLUSION

For two-factor authentication, Time-based One-Time Passwords (TOTP) are an excellent option. It uses software to generate code and is entirely dependent on open-source projects. It doesn't require any kind of proprietary software or hardware, such those offered by VeriSign and RSA Secure ID. Additionally, everything is completed offline. It can be implemented in a variety of computer languages and is a stand-alone program. Time-based One-Time Password (TOTP) generation employing the HMAC technique combines a secret key and hash for a certain time slot to produce an OTP. It confirms the validity and integrity of data, giving user's additional peace of mind that they are who they say they are. The increasing frequency of security breaches and exposed information necessitates the use of multifactor authentication. One efficient and straightforward method of adding two factor authentications (2FA) to a system is through the use of time-based one-time passwords (TOTP). Even while the method is very safe by itself, there are a number of other things that can go wrong, such as losing the secret key.

REFERENCES

[1]. AmjadAbdallahAbdelkarim, Hebah H. O. Nasereddin, "Intrusion Prevention System International Journal of Academic Research Vol. 3. No.1 January, 2011, Part IIBurger, J. 2008.
[2]. Hussain Ahmad MadniUppal ,MemoonaJaved and M.J. Arshad "An Overview of Intrusion Detection System (IDS) along with its Commonly Used Techniques and Classifications"International Journal of Computer Science and Telecommunications, Volume 5, Issue 2, February 2014.
[3]. https://www.secureworks.com/blog/the-evolution-of-intrusion-detection-prevention.
[4]. Jilliang Zhang, Xiao Tan, XiangqiI Wang, Ainin Yan, and Zheng Qin "T2FA: Transparent Two-Factor Authentication" IEEE accepted June 2,2018, date of publication June 15, 2018, date of current version July 6, 2018.
[5]. KavithaBoppudi "Efficient HMAC Based Message Authentication System for Mobile Environment" Global Journal of Computer Science and Technology Volume 11 Issue 19 Version 1.0 November 2011.
[6]. Mark Lutz, 2013, Learning Python, Fifth Edition.
[7]. PHP Cookbook Book by Adam Trachtenberg and David Sklar, 2002, Third Edition.
[8]. Chaitya B. Shah, Drashti R. Panchal "Secured Hash Algorithm-1: Review Paper" International Journal Of Advance Research in Engineering And Technology Volume 2, Issue X, Oct 2014.
[9]. https://brilliant.org/wiki/secure-hashing-algorithms/.
[10]. Dr. S.Vijayarani1 and Ms. Maria Sylviaa.S "Intrusion Detection System – A Study" International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015
[11]. Raaed K. Ibrahim, Ali SH. Hussain, Roula A. Kadhim," Implementation of Secure Hash Algorithm By Labview" IJCSMC, Vol. 4, Issue. 3,March 2015, pg.61 – 67.
[12]. Neha Kishore, Member IAENG, and Bhanu Kapoor "Attacks on and Advances in Secure Hash Algorithms" IAENG International Journal ofComputer Science, 43:3, IJCS_43_3_08.