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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 2, February 2019

Network Intrusion Prevention System

Ayush Gupta[1], Shreyash Ninawe[2], Vilas Bariyekar[3], Ranjita Asati[4]

Priyadarshani Institute of Engineering and Technology, Nagpur, India[1,2,3]

Assistant Professor, Department of Computer Science and Engineering,

Priyadarshani Institute of Engineering and Technology, Nagpur, India[4]

Abstract: The area of intrusion prevention is the central concept in overall network and computer security architecture. It is an important technology in business sector as well as in research area. By monitoring the computer and network resources, Intrusion Prevention System (IPS) prevents any of the misuse or unauthorized access which is basically an attack to these resources. Here we have implemented the application of Two-factor authentication through which the one time password is generated at the host side itself instead of the server's. Which is hence impossible to intrude? And also, it is re-created in a certain time interval without any interference of external means. So, it is a easy way of accessing our accounts. We have implemented this with the help of SHA algorithm in this paper, we have discussed the introduction of intrusion prevention system This paper will be helpful for the new researchers who want to know the basic knowledge of intrusion prevention systems.

Keywords: TOTP, SHA-1, HMAC, Google Authenticator.

I. INTRODUCTION

With the explosion in Internet connectivity and the mainstream use of broadband and mobile technologies, there has been a huge increase in the number of computer systems and storage devices connected to the public network. With an ever-increasing reliance on computing infrastructure, we find that our critical IT assets, confidential data and intellectual property are more susceptible to cyber attack than ever before. In response to the changing threat landscape, Network Intrusion Prevention Systems was developed to provide advanced protection beyond that offered by firewalls and Intrusion Detection Systems. Firewalls and Intrusion Detection Systems provide security but do not arrive the point that Intrusion Prevention System provides.
According to Hussain [2] The process of preventing the events occurred in a computer system or network resources, then analyzing them for the indications of intrusion and probable incidents that can cause threats to security measures, is called Intrusion Prevention. Intrusions are usually caused by intruders/attackers, who want unauthorized and additional privileges to particular system or network for their own purposes. IPS is a new technology that provides security for computer systems with new features that are effective in facing threats. IPS can considered as important component in any IT system defense. There are many reasons that IPS considered like that, among that it protect from denial of service attacks and protect any weakness points in any software. The features of IPS are used in large organizations and the individual users in homes began to use it There are many types of IPS that practice in many areas, these types are inline network intrusion detection system, application-based firewalls/IDS, layer seven switches, network-based application IDSs, deceptive applications.

According to Amjad [1] IPS is a system that protects the following: -
Confidentiality: that it protect the information that stored on a computer and it prevent unauthorized use of that information (Viewing or Copying).
Integrity: IPS protects the integrity of information and prevents the alteration on that information from unauthorized users.

II. RELATED WORK

In [10] Dr. S.Vijayarani stated that, An Intrusion Prevention System (IPS) is a network security/threat prevention technology that audits network traffic flows to detect and prevent vulnerability exploits. There are two types of prevention system they are Network (NIPS) and Host (HIPS). These systems watch the network traffic and automatically take actions to protect networks and systems. IPS issue is false positives and negatives. False positive is defined to be an event which produces an alarm in IDS where there is no attack. False negative is defined to be an event which does not produces an alarm when there is an attacks takes place. Inline operation can create bottlenecks such as single point of failure, signature updates and encrypted traffic. The actions occurring in a system or network is measured by IDS.

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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 2, February 2019

According to Hussain in [2] We have seen a lot of improvements to IDS/IPS products. They all are still quite similar to their original incarnation, which started with an academic paper written in 1986. The IDS/IPS basic fundamentals are still used today in traditional IDS/IPSs, in next generation intrusion prevention systems (NGIPSs) and in Next-Generation Firewalls (NGFWs). The Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) started with an academic paper written by Dorothy E. Denning titled "An Intrusion-Detection Model," which led Stanford Research Institute (SRI) to develop the Intrusion Detection Expert System (IDES). That system used statistical anomaly detection, signatures and profiles of users and host systems to detect nefarious network behaviors. To this day, intrusion detection and prevention systems (IDS/IPS) are changing and will likely continue to change as threat actors change the tactics and techniques they use to break into networks. Thus far, we looked at how an academic paper birthed the IDS/IPS concept and changed over the years until 2005. In [9] this has been examined that In 2008 hackers were using iFrame redirects on popular websites like news sites to redirect a user to the hacker's site. If end users had vulnerabilities in their applications or web browser when they landed on one of those popular sites the Iframe code would redirect them to a malicious website. This required IDS/IPS vendors to provide additional countermeasures. In addition to pattern matching, string matching, anomaly detection and heuristic based detection, vendors added information to block malicious command & control IP addresses as well as websites that were known to host malware, reducing the time it takes to detect threats. Another addition to IDS/IPS came about after the 2011 breach on RSA, the security company widely known for its two-factor authentication product. They began using MD5/SHA checksums of known bad files. Each file has a unique checksum. Checksums (also known as hashes or signatures) are strings of characters made from numbers and letters, which can be used to verify the integrity of files and text messages. If the checksum that entered the network matched the checksum the vendor had on file, the sandbox would alert the victim's organization that malware had just entered the network. Back then, this was a milestone for protecting network. Today, this type of technology is being used in NGFWs. To overcome this issue cryptogaphy key came into existence.

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 takes a variable sized input message and produces a fixed-sized output. The output is usually referred to as the hash code or the hash value or the message digest, hash functions play a significant role in today's cryptographic applications. SHA (Secure Hash Algorithm) is a famous message compress standard used in computer cryptography, it can compress a long message to become a short 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). SHA stands for Secure Hash Algorithm, the four algorithms for secure hash functions SHA-0,SHA-1 ,SHA-2 and SHA-3 .SHA-1 is very similar to the standard SHA-0 but corrects an error in the original SHA hash specification that led to significant weakness , SHA-1 was first originated in 1995 and currently the most widely used SHA hash function. It is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP. In [12] A cryptographic hash function must be able to withstand all known types of cryptanalytic attack. At a minimum, it must have the following properties of a secure cryptographic function: The CHF H can be applied to a block of message of an arbitrary length. 1. It produces an output h of fixed length. 2. It is relatively easy to compute h for a given M. 3.Pre-image Resistance: Given h, it is infeasible to generate M such that H(M)=h. 4.Second Preimage Resistance: Given M, it is hard to find another message, M", such that H(M)=H(M"). 5.Collision Resistance: Given M≠M", it is infeasible to find H(M)=H(M"). 6.Pseudo-randomness: The value h must be deterministic and it must random in relation to its input. In recent years, there has been great development in CHFs that satisfy these properties. A CHF that satisfies the above stated first five properties are referred to as a weak hash function. One of the simplest hash function [1, 57] uses bit by-bit exclusive-OR (XOR) of the data for every block of the message and combines it with a one-bit circular shift or rotation of the resulting hash code for each block. Although this procedure gives a good measure of data integrity, ideally it doesn't provide enough security in terms of collision protection when the encrypted hash value on a simple plaintext message. The most widely used CHF have been the Secure Hash Algorithm (SHA) and the Message Digest (MD) family. We mainly look into the SHA family in this paper. The MD family algorithms also have a structure that is similar to the SHA family algorithms.

III. METHODOLOGY

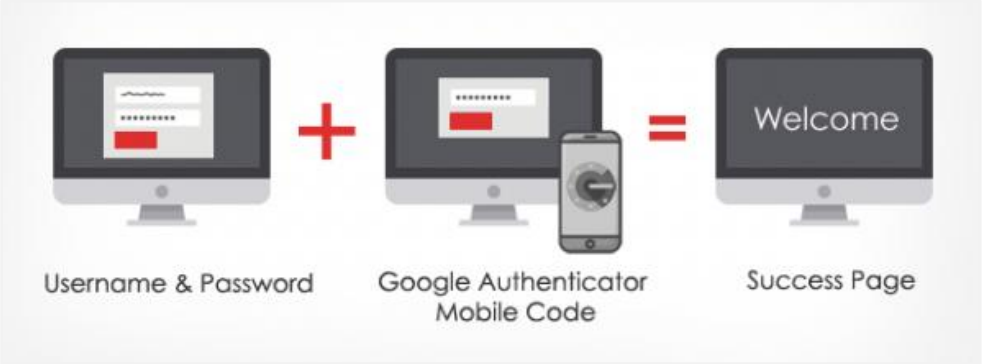
Secure Hashing Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash function SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 2, February 2019



Two-factor authentication (2FA), sometimes referred to as two-step verification or dual factor authentication, is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access. Two-factor authentication provides a higher level of assurance than authentication methods that depend on single-factor authentication (SFA), in which the user provides only one factor -- typically a password or passcode. Two-factor authentication methods rely on users providing a password as well as a second factor, usually either a security token or a biometric factor like a fingerprint or facial scan.

In two factor authentication(2FA) we use Secure Hash Algorithm(SHA) to generate a four digit code which will be time dependent and will change after every 30 seconds. The Secure Hash Algorithms are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS).

Secure Hash Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. The hash function then produces a fixed-size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they're transformed into their respective hash values, it's virtually impossible to transform them back into the original data. A few algorithms of interest are SHA-1, SHA-2, and SHA-3, each of which was successively designed with increasingly stronger encryption in response to hacker attacks. SHA-0, for instance, is now obsolete due to the widely exposed vulnerabilities.

A common application of SHA is to encrypting passwords, as the server side only needs to keep track of a specific user's hash value, rather than the actual password. This is helpful in case an attacker hacks the database, as they will only find the hashed functions and not the actual passwords, so if they were to input the hashed value as a password, the hash function will convert it into another string and subsequently deny access. Additionally, SHAs exhibit the avalanche effect, where the modification of very few letters being encrypted causes a big change in output; or conversely, drastically different strings produce similar hash values. This effect causes hash values to not give any information regarding the input string, such as its original length. In addition, SHAs are also used to detect the tampering of data by attackers, where if a text file is slightly changed and barely noticeable, the modified file's hash value will be different than the original file's hash value, and the tampering will be rather noticeable.

IV. OVERVIEW OF TOTP

User authentication is to establish the trust between users and devices and has become the most forefront defense for cyber-security. The static single-factor authentication such as ''username + password'' has been used widely because it is easy to deploy without additional devices. According to Jiliang [4] However, the security of single-factor authentication depends on the password. Such authentication is effective in the early Internet, where remote access was not used widely and the attack pattern was single. Nowadays, Trojans are able to intercept the user's keyboard record and even decrypt the user's login account and password by collecting the location clicked by the mouse, thus breaking the password protection technology.

In order to enhance the security, Two-Factor Authentication (2FA) was proposed. 2FA is a method of confirming a user's claimed identity by utilizing a combination of two different factors: 1) something they know, 2) something they have, or 3) something they are, i.e., a combination of passwords and physical entities such as smart cards, mobile phones, tokens, or fingerprints. However, compared with the password-based single-factor authentication, two-factor authentication brings inconvenience to users when a physical entity is used as the second authentication factor, where many additional operation steps are added. For example, the dynamic token method is a one-time password and provides the high security, but it requires carrying different tokens when the user visits different sites.

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

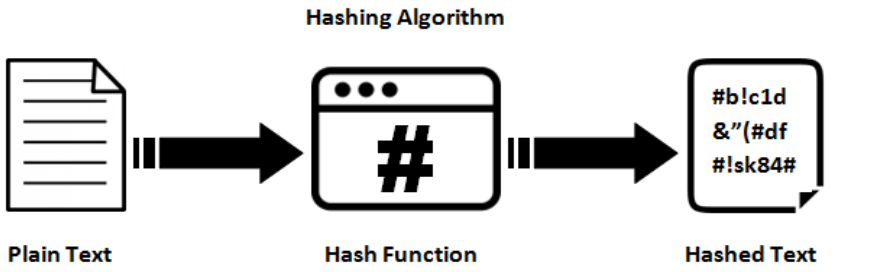
IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 2, February 2019

According to Jiliang [4] The second factor authentication is completely transparent to the user, avoiding the tedious interaction between the user and the device. Therefore, our proposed T2FA exhibits the anti-fraud ability with good application prospect.

Secure Hashing Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash function SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.



V. DISCUSSION AND CONCLUSION

Time-based One-Time Password (TOTP) is a great way to do two-factor authentication. It is totally based on open source project and generates code with the help of software. It does not need any type of proprietary hardware or software solution, such as provided by RSA SecurID and Verisign. And everything is done offline. It is an independent program and can be implemented in a no of programming languages.

In Time-based One-Time Password (TOTP) generation using HMAC algorithm we are combining a hash with a secret key for a particular time slot that generates One-time password (OTP) .It verify data integrity and authenticity, thus provide extra assurance that users are who they claim to be. With the growing rate of security breaches and information being compromised, multi factor authentication is the need of the hour. Time-based one-time password (TOTP) can be considered as an effective and simple way of implementing 2 factor authentication(2FA) on a system. Though, the algorithm is quite secure in itself but there are various other factors that make it vulnerable like losing secret key etc.

REFERENCES

[1]. Amjad Abdallah Abdelkarim, 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 Madni Uppal , Memoona Javed 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]. Kavitha Boppudi "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 of Computer Science, 43:3, IJCS_43_3_08