IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 12, December 2017

Ensuring Efficiency of Authentication by Providing Redundant Authentication by using Dynamic Password Methods using BCrypt Algorithm in VPN Access

Dr. S. Yamini[1], M. Anbunesan[2]

Director, School of Computer studies, Rathnavel Subramaniam College of Arts and Science, Coimbatore, India[1]

Asst., Professor, School of Computer Studies, Rathnavel Subramaniam College of Arts and Science, Coimbatore, India[2]

Abstract: As networks become borderless in modular times, the accessibility of networks are also increasing in proportionate to its growth. Enterprises have employees and partners who often needed to access their corporate resources from their respective remote location keeping in mind about the confidentiality, integrity and availability of the data throughout the whole access phrases. Borderless networks encourage and promote the growth of secured remote access to corporate resources to their remote employees and partners. In modeler times out of several remotes access methods, VPN is one of the most used methods that provide C.I.A (confidentiality, integrity, availability) factors. Traditional VPNs supports the C.I.A factor with the help of only predefined authentications, possibly in certain cases linked with third party authorized authentication servers. In this work it has been proposed to use VPN in traditional way but added with an extra Layer of authentication name called 2 step authentications which involves the use of dynamically generated OTP/OTAC with Bcrypt Algorithm. The remote user/partner needs to pan the traditional authentication along with the 2nd step verification before the private access is granted to him/her.

Key words: C.I.A - Confidentiality, Integrity, and Availability, , VPN, OTP/OTAC

I. INTRODUCTION

When considering network, you can view them from different perspectives. For example, senior organization might view the network as a business tool to simplify the goals of the company. Network technicians (at least some) might ponder their networks to be the center of the universe. End users might consider the network to be just a tool for them to get their work done, or possibly as a source for restoration. Not all users escalate their role in keeping data safe, and tactlessly the users of the network represent a significant vulnerability, in that they have usernames and passwords(or other credentials, such as one-time password token generators) that allow them contact to the network. If a user is cooperated or an unauthorized individual gains access, the security of the network may still fail as a result, even after you apply all the concepts that you learn in this project. So, an important point to remember is that the users themselves represent a security risk and that training users is a key part of a comprehensive security policy.

Confidentiality, Integrity, and Availability

Network security objectives usually involve three basic concepts:

1. Confidentiality: There are two types of data in wave as it moves across the network; and data at rest, when data is being on storage media (server, local workstation, in the cloud, and so forth). Confidentiality means that only the trusted individuals/systems can view delicate or classified information. This also suggests that untrusted individuals should not have any type of access to the data. Concerning data in motion, the primary way to protect that data is to encrypt it before sending it over the network. Another option you can use with encryption is to use distinct networks for the transmission of intimate data.

2. Integrity: Integrity for data means that changes made to data are done only by trusted individuals/systems. Corruption of data is a failure to maintain data integrity.

3. Availability: This applies to systems and to data. If the network or its data is not available to trusted users possibly because of a denial-of-service (DoS) attack or maybe because of a general network failure the impact may be noteworthy to companies and users who trust on that network as a business tool. The failure of a network generally likens to loss of income. Cost-Benefit Analysis of Security Network security engineers must know not only what they protect, but also from whom. Risk management is the key phrase that you will hear over and over, and although not

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 12, December 2017

very trendy, it is based on specific ethics and concepts related to both asset protection and security management. A threat is any budding danger to an asset. If vulnerability exists but has not yet been exploited, the threat is c and not yet realized. If someone is actively launching an attack against your system and successfully accesses something or compromises your security against an asset, the threat is realized. The entity that takes advantage of the vulnerability is known as the threat agent or threat vector. A countermeasure is a safeguard that somehow mitigates a potential risk. It does so by either reducing or rejecting the vulnerability, or at least reduces the odds of the threat agent to actually exploit the risk.

II. OVERVIEW OF THE VPN

Now a day in computer world, security is the most challenging thing one. So we are in need to secure our data while transpiring by using any network. Our thesis covers only a VPN based networks. In this project we are having around eight chapters for describe the project step by step. Chapter one and two for introduction about the project and literature serve. In literature serve chapter we discussed nearly around ten various papers which is related to VPN network based projects. Chapter three problem definitions which is include existing system and proposed systems. And chapter four is system methodology which is containing requirement descriptions of deploying Remote access VPN networks. Hardware, software, tool regiments.

Chapter five describe about the system design its describe about what topology we are going to implement in this project and how they connected each other's, OTP server configurations , VPN firewall and server configurations.

Chapter six contains system implementations. Configuring topology assigning IP address, Routing protocol configurations, ACL (Access Control List) creations, firewall configurations, VPN profile creations, VPN Clint creations, OTP server deployment.Anyconnect software configurations in client systems or mobiles.

Chapter seven discus about the final result of our project and conclusion of project. Finally future enhancement of our project. Chapter eight display our screen shot of our project and coding, configurations commands. What are all the papers we were studied to do our project we are going to tell as a references of our project

The VPN network are two types,

1. Site-to-Site VPN
2. Remote VPN network.

We mainly focus into Remote access VPN networks. Because the Site-to-Site VPN networks transferring data or connecting each other inside its own sites so there is less chance to happening any attacks or any vulnerability. But in remote access VPN there is many chance to happening attacks or any vulnerability.

Our thesis motto is to increase the security level in remote access VPN networks. In that case we are going to use 2 step authentication to secure the remote access VPN.

III. PROBLEM DEFINITION

Problem

VPN authentication is currently on pre-defined pass phrase (password) only. So, attack on the authentication session is still possible by manipulating the stored credentials on the VPN authenticating server or VPN Concentrator. This vulnerability mostly affects the roaming employees/business partners as they are mostly using RA VPN access.

Mostly all VPN networks using username and passwords authentications which is provided by the system administrators so there is may be chance to attack your connections internally. And the second chance is if your connection with your private network using public network, in that public network there is so many attackers being there if you trying to connect using username and password they can easily get your login details and they can use that details in future because that username and passwords are static once your created it won't be expired once you change by yourself.

Suggested Solution

To authenticate the VPN accesses using pre-defined passwords with login ID along with using a 2 step verification method. As far as 2 step verification is concerned best method is to use OTP that will be generating in a random manner and also the whole process can be linked with Single Sign On facilities in terms of access all other internal resources of the organization by the Remote User. 2 step based authentication can only be applicable for SSL based RA VPN connection only as they are mostly used by roaming employees or business partners.

BCRYPT ALGORITHM

Generally, user selected passwords are hashed and keeping in to database. Hashed passwords are then encrypting using cryptography algorithm. Characteristic hash functions are known as MD5, SHA1 and SHA256. Hash passwords are the vulnerable to Dictionary table attacks and Brute Force Attacks. Presentations of hash process are vast in cryptography and software design repetition. Encryption and hash process are two connected and harmonizing arenas are not

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 12, December 2017

additional technologies for one extra. PBKDFs are commonly intended to be computationally uncaring, that was took moderately long time to calculate. It is tough for the hackers to repossess the password. Hashing algorithms also used for charting of variable span data to static output, recovering the data from the database else data lookup. Cryptographic hash purposes are used for structure hunks for HMACs which offers message authentication. They confirm honesty of data that is conveyed. If x and y are efforts such that H (x) =H (y), and x • y.

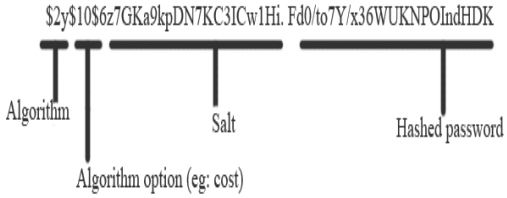

Fig : 3.1 PBKDF

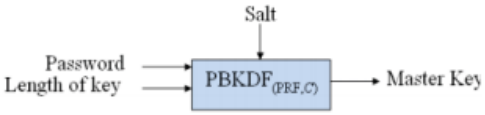

Fig : 3.2 Bcrypt Algorithm

Bcrypt has exclusive key setup programme, cross podium encryption service. Bcryptuses EBC (Electronic Code Block) and is also cross podium encryption service. Bcrypt divides the input value into sub keys and flinches block encryption of the sub keys. The subsequent is encrypted sub keys affixed.

IV. RELATED WORKS

OlalekanAdeyinka (2008) examined the security issues of IPsec VPN technology with respect to remote access communication. The opening or ports on the firewall may present a security breach, as it opens the door through which malevolent users can enter the entire network. Yongtao Wei et al (2008) have presented the design and evaluation of a service prototype over a virtual network, which provided a bandwidth guaranteed multi-path routing with a bandwidth allocation algorithm. Their evaluation showed that the packet loss rate, throughput and bandwidth utilization of traffic using BGMR, was much better than that of OSPF. Their simulation experiments showed a massive increase in throughput with that of low loss broad-mindedness and resource utilization compared with that of the conservative routing protocol OSPF.

Friedrich Eisenbrand et al (2007) have suggested three main contributions: (1) they provided a new and significantly stronger lower bound on the cost of an optimum solution. (2) They presented a new randomized approximation algorithm. (3) Their VPND algorithm used a Steiner tree approximation algorithm as a subroutine. To the best of their knowledge, this is the first time that a nontrivial result from a precise algorithm led to an improved polynomial-time guesstimate algorithm.

Benhaddou et al (2006) presented a novel control scheme for shared L1-VPN operation in multi-domain networks and derived both integrated and distributed variations. They analyzed the performance evaluation of the resource management model, namely, dedicated and shared L1-VPN. The resulting gain in carried load is dependent upon VPN topologies, traffic demands, and inter-VPN or non-VPN link overlaps. The results showed that allocated control provides better network utilization and shared L1-VPN increases network utilization.
Haibo Wang and Gee-Swee Poo (2006) have investigated the problem of the availability of guaranteed service provisioning in hose model VPNs. They showed that the problem is NP-complete and proposed a multipath routing experiential to solve it. Their solution elegantly solved the too- 17 many-path problem encountered in their works in literature and the related

REFERENCES

[1] https://www.youtube.com/watch?v=1oJ1JwYAC8w
[2] https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html.
[3] M. Abdelhakim, J. Ren, and T. Li, "Mobile access coordinated wireless sensor networks –topology design and throughput analysis," IEEE Global Communications Conference, GLOBECOM'13, pp. 4627–4632, Dec. 2013.
[4] E. J. Duarte-Melo and M. Liu, "Data-gathering wireless sensor networks: organization and capacity," Computer Networks,vol. 43, no. 4, pp. 519–537, 2003, wireless Sensor Networks.
[5] W. Liu, K. Lu, J. Wang, G. Xing, and L. Huang, "Performance analysis of wireless sensor networks with mobile sinks," IEEE Transactions on Vehicular Technology, vol. 61, no. 6, pp. 2777–2788, Jul. 2012.
[6] I. Maza, F. Caballero, J. Capitan, J. Martinez-de Dios, and A. Ollero, "A distributed architecture for a robotic platform with aerial sensor transportation and self-deployment capabilities," Journal of Field Robotics, vol. 28, no. 3, pp. 303–328, 2011.