RESEARCH ARTICLE OPEN ACCESS

Network Security Based on Authentication Techniques

J.Revanthraj [1], T.Sathyabama [2]
Department of Computer Application (PG)
Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore
Tamil Nadu -India

ABSTRACT
Network Security is a problem of square measure currently changing into vital as society is moving to digital modern era. knowledge security is that the almost essential part in guaranteeing safe transmission of data through the web. It contains authorization of access to data during a network, controlled by the network administrator. The task of Network security not solely needs guaranteeing the safety of finish systems however of the complete network. Authentication is one in every of the first and most ordinarily ways in which of ascertaining and guaranteeing security within the network.
***Keywords*:-** service of denial, virtual network, password, RSA.

I. INTRODUCTION

In this digital era additional and additional folks changing into active on the web for his or her personal and skilled, as a result of this net is growing chop-chop. But, together with the evolution of Networking and net, many threats like Denial-of-Service (DOS) attacks and Trojan Horses have conjointly up drastically. that the task of securing the web or perhaps the native space Networks is currently at the forefront of network connected problems. Being on public network, serious security threats may be posed to associate degree individual's personal info and conjointly to the resources of firms and government.

II. DATA SECURITY AND AUTHENTICATION

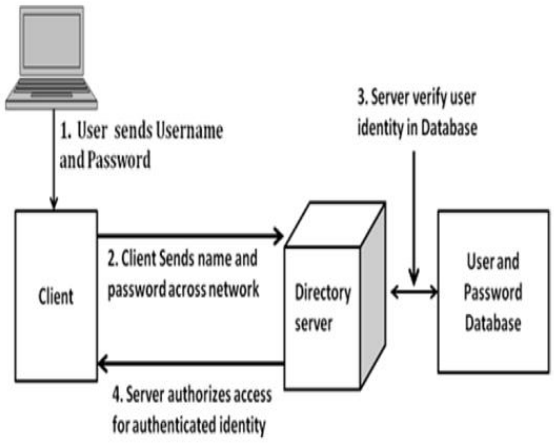
Data Security could be a difficult issue within the field of knowledge communications. For securing data from hackers and haywire, authentication is that the major introduce network security. it's an idea to shield network and information transmission over wired in addition as wireless networks. Authentication is one in all the first techniques of guaranteeing that the one that is transmission the data is whom he says he's.

it's so the method of decisive the particular identity of users, systems or the other entity in network.

III. AUTHENTICATION TECHNIQUES

A. *PASSWORD AND PIN BASED:*

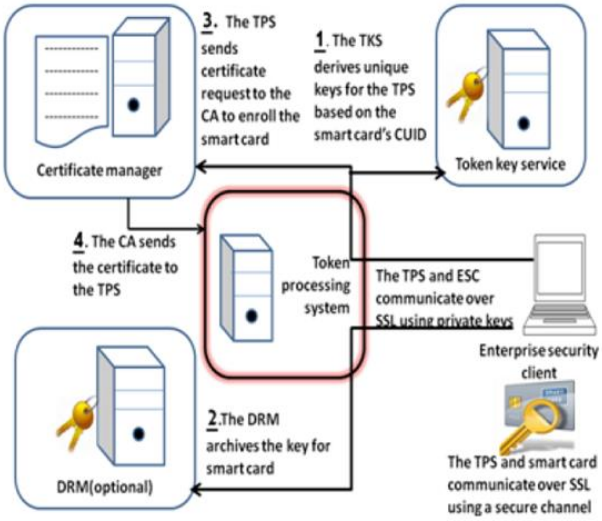
In this authentication technique, privacy and confidentiality is maintained up to some extent. Users study there passwords and therefore we will term these as Knowledge-based techniques. Passwords is single words, numeric, phrases, any combination of those or personal positive identification. however drawback with this system is that memorized passwords is simply guessed or arbitrarily searched by the hackers. Virtual personal Networks like Point-to-Point Tunneling Protocol (PPTP) create use of each clear-text protocols like parole Authentication Protocol (PAP) and MD5-based protocols like Challenge shake Protocol (CHAP).



Directory Server based authentication

B. *TOKEN BASED:*

This is a physical device that performs authentication and thus will be termed as object primarily based. Tokens will be compared with physical keys to homes that ar used as a token however in digital tokens several alternative factors ar gift to supply data safety. In digital world, security tokens ar used. Tokens themselves have countersign thus not withstanding they're lost, the hackers cannot modify the very important data. Bank cards, sensible cards are security token storage devices with passwords and pass codes. Pass codes ar same as countersign except that the previous ar machine generated and keep. There exist just once security tokens and smartcards.



Token-based (Smart Card) Authentication in Certificate System.

C. *BIOMETRIC BASED:*

Biometric authentication is that the method of confirming if a user is whom he's claiming to be, mistreatment digitized biological signatures of the user. biometric identification may be classified into 2 groups: physiological and activity. In physiological authentication, faces, finger prints, hands, iris and tissue layer follow. And within the case of voice prints, signatures and keystrokes area unit used. this system will term as ID based mostly. this system is safer as compared to parole and token based mostly techniques. biometric identification techniques area unit presently operative in numerous enterprises. they're used for passports, visas, personal identification cards, accessing bank machines, entry access management, and general pc desktop access.

IV. COMPARSION OF STRENGTH OF PARAMETER OF AUTHENTICATION MECHANISM

For examination the on top of 3 authentications, we tend to think about 3 vital factors shown within the Graph one and eventually calculate the composite of all those factors to work out the Binding strength that becomes the only purpose of comparison.

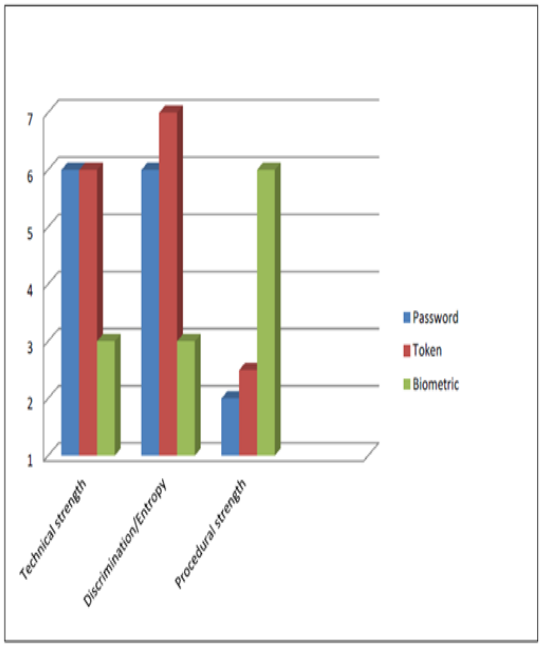
But, the model that we tend to use to search out this worth makes use of individual weaknesses instead of individual strengths wherever weakness = 1/strength. As a result, we tend to get the subsequent equation:

Binding Weakness = Discriminatory Weakness + Procedural Weakness + Technical Weakness

1. Discrimination Strength: For passwords, range of makes an attempt in an exceedingly outlined period of time. just in case of tokens, we tend to think about their distinct range.

2. Technical Strength: For all the 3 authentication mechanisms, security analysis method is disbursed.

3. Procedural Strength: this can be onerous to work out because it could rely on several environmental factors like website security and employees discipline. But, still we tend to use a particular set of parameters to determine the worth like length, randomness and frequency of modification within the case of Passwords; physical security and user discipline within the case of Tokens and for life science, inherent strength is spare.



Comparison of strengths of different parameters of authentication techniques

V. MULTI FACTOR AUTHENTICATION

To make network safer, a mixture of higher than techniques ought to be used as four. This is often noted as multi-factor authentication. For network security, every appraiser result should be glad. As a Boolean AND operation is performed for every factor's authentication results, thus all should be affirmative. 2 issue authentications in ATM cards area unit the cardboard itself and its watchword. thus notwithstanding the cardboard was lost or purloined, we will make sure that the security is maintained till hackers don't apprehend cards watchword. This instance of token and watchword area unit largely enforced these days.

VI. CONCLUSION

Network security are often maintained by creating use of assorted authentication techniques. User needs to use authentication technique betting on demand. Positive identification primarily based technique is best if you have got to recollect one positive identification. we got to bear in

mind several passwords thus we use those passwords that square measure simple to recollect.

REFERENCES

[1] R. Dhamija, and A. Perrig,"Déjà Vu: "*A User Study Using Images for Authentication*", 9th USENIX Security Symposium, 2000.

[2] R. Morris, K. Thompson, "*Password security: A case history*," Comm. ACM,

[3] B. L. Riddle, M. S. Miron, J. A. Semo, "*Passwords in*

[4] S. M. Bellovin, M. Merritt, "*Encrypted key exchange: Password-based protocols secure against dictionary attacks*," Proc.

[5] S. M. Furnell, P. S. Dowland, H. M. Illingworth, P. L. Reynolds, "*Authentication and supervision: A survey of user attitudes*," Computers and Security, Vol. 19, no.6, 2000.

[6] Harbitttr, A. and Menasce, D.A., "*A Methodology for Analyzing the Performance of Authentication Protocols*", November 2002.

[7] Haq, I. U. and Yahya, K. M. "*Heterogeneous Networks: Challenges and Future Requirements".*

[8] TSENG, Y.M., YANG, C.C. AND HAUR SU, J. *"Authentication and Billing Protocols for the Integration of WLAN and 3G Networks*", 2004.

[9] Li, S., Zhou, J., Li, X. and Chen, K.

[10] Misbahuddin, M., Premchand, P. and Govardhan, A. "