International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com, Special Issue 42 (AMBALIKA) (March 2017), PP. 35-39

AN ANALYSIS ON THE SECURITY OF NETWORK BASED ON AUTHENTICATION TECHNIQUES

[1] 1Devendra Kumar, [2]Sarika Tyagi, [3]Himanshu Kumar Shukla
[1,3] Department of Computer Science and Engineering, AIMT, Lucknow, India
[2] Department of Computer Science and Engineering, RKGIT for Women, Ghaziabad
[1] devendrakumar17@gmail.com, [2] sarikatyagi26@gmail.com,[3] himanshu0590@gmail.com

***Abstract*— Network Security issues are very important issues in now days as society are moving to digitalization. Security of data is the most critical component to ensure secure transmission of data through the internet. It contains the authorization of access to data in a network that is controlled and managed by the network administrator. Network security not only requires ensuring the security of clients of a network but of the whole network. Authentication is one of the primary and most commonly way to ascertain and to ensure the security in the network. In this paper, we are attempting an analysis on the various authentication techniques. These Authentication techniques are Token- based, Knowledge-based and Biometric-based etc. After this, we will consider multi-factor authentications by making a combination of above authentication techniques and try to compare those.**

***Index Terms*—** Authentication Techniques; Integrity; Token; Pass code; Smart card; RSA; Denial of Service; Biometric.

I. INTRODUCTION

In this digital age people are becoming more active on the Internet day by day for their personal and professional, because of rapidly growth of the internet. But, along with the development of Networking and Internet, several threats such as DOS (Denial-of-Service) attacks and Trojan horse have also risen drastically. So the job of securing the Internet or even the Local Area Networks is now in the front of issues related to computer network.

In a network serious security threats can be determined to an individual's personal information and also to the resources of a company and government. Providing confidentiality, to maintain integrity and to assure the availability of correct information these are the primary objectives of Network Security.

These threats are founded in a network due to the irresponsibility of the users, used old technology and poor security management of the network.

Sometimes in a network there are some network services that are enabled in a personal computer or a router by default. But among those enabled services some are not necessary and can be used by an attacker for information collection.

So it is necessary to disable these unused services to protect the information from hackers.

While developing a secure network, the following points are needed to be considered –

1. Access – Only authorized users should be allowed to access a particular network.
2. Authentication – It is the process of identifying whether someone is, in fact, who are what it is declared to be. Real flow of information will start only after the user has been authenticated and allowed to communicate in the network.
3. Confidentiality – Confidentiality is equivalent to privacy. It is used to assure that the information can be accessed only by authenticated user and it is achieved by using encryption.
4. Integrity – It involves maintaining the accuracy, consistency and trustworthiness of data over entire network.

II. AUTHENTICATION AND DATA SECURITY

Data Security is a challenging issue for data communications over a network. To secure data or information from hackers, authentication plays a very important role in network security. It is a technique to secure a network and transmission of data over wired as well as wireless networks. Authentication is process of determining whether someone is, in fact, who are what it is declared to be.

To verify someone's identity, password is mostly used technique. For user or machine's authentication, different authentication techniques are used to perform authentication between user and machine or machine and another machine too.

Different types of attacks may be occur during authentication is shown in Table I.

Table I
Different Types of Attacks on Network/Data

Types of Attacks	**Description**
Weak password recovery	Websites permit users to illegally obtain, modify or recover password of another user.
Brute force attacks	By trial and error, hackers try to guess userid, password, card numbers, etc. This technique is highly popular.
Inadequate authenticati on	Some websites don't have best authentication technique so hackers attack on us
Shoulder surfing attacks	The attackers use observation technique such as looking over someone's shoulder

A. Password and pin based Authentication:

In password & pin based authentication technique, confidentiality and privacy is maintained up to some extent. Users memorize their passwords and hence we can call this as Knowledge-based technique. Passwords can be single word, numeric, phrases, any combination of these or personal identification number. But problem with this technique is that passwords can be randomly searched or easily guessed by the hackers.

Virtual Private Networks such as PPTP (Point-to-Point Tunneling Protocol) make use of both clear-text protocols such as MD5-based protocols and Password Authentication Protocol (PAP) and like Challenge Handshake Protocol (CHAP). MD5-based protocols should be preferred due to sniffing attacks. Plain passwords should be avoided for security purpose. Plain passwords must be used only with SSL (Secure Socket Layer) certificates.

III. AUTHENTICATION TECHNIQUES

Following are the primary authentication techniques used in the public network thesedays:

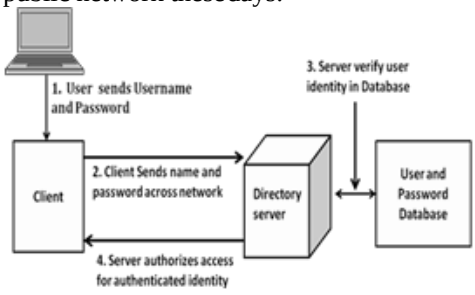


Fig. 1 Directory Server based authentication

Fig.1 is showing working of password based authentication technique. User first enters a username and password. In directory server based authentication the Client application binds itself to the Directory Server with a different Name. The client retrieves domain name by using the name entered by user. After that the client sends these credentials to the Directory Server and then server verifies that password which is sent by the client by matching it against the password stored in database. If password matches, the server accepts the credentials for authenticating the user's identity.

A. Password and pin based Authentication:

In password & pin based authentication technique, confidentiality and privacy is maintained up to some extent. Users memorize their passwords and hence we can call this as Knowledge-based technique. Passwords can be single word, numeric, phrases, any combination of these or personal identification number. But problem with this technique is that passwords can be randomly searched or easily guessed by the hackers.

Virtual Private Networks such as PPTP (Point-to-Point Tunneling Protocol) make use of both clear-text protocols such as MD5-based protocols and Password Authentication Protocol (PAP) and like Challenge Handshake Protocol (CHAP). MD5-based protocols should be preferred due to sniffing attacks. Plain passwords should be avoided for security purpose. Plain passwords must be used only with SSL (Secure Socket Layer) certificates.

System catalogs are used to store passwords for every user in database where we use commands like CREATE USER, CREATE and ALTER ROLE to manage those passwords. For example, CREATE USER jacks WITH PASSWORD information. If there is no password has been set up for a user, then stored password will be NULL and password authentication will be failed for that user.

In password-based authentication techniques, there are some password policies are used, this password policies are created by using a set of rules that also have major roles in deciding how to administer manage the authentication in the systems also in the network. There are multiple password policies which are supported by the directory servers, "Specialized" and "Default". The password policy "Default" can be classified in the configuration entry, it applies to all the accounts in directory server. The password policy "Specialized" can be configured for an individual user or a set of users by using role and CoS feature.

B. Token based Authentication:

Token based authentication is a physical device which performs authentication and

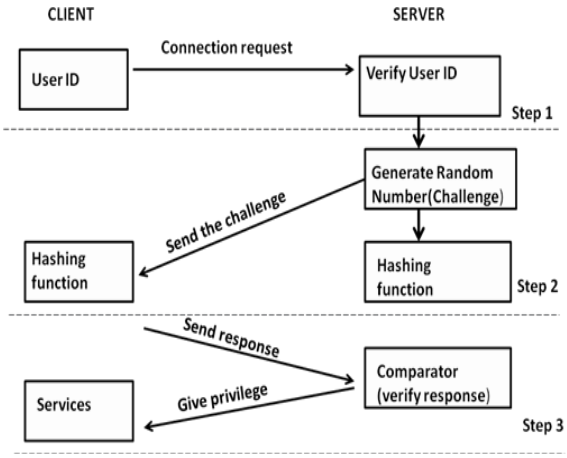


Fig. 2 Token-based (Smart Card) Authentication in a Certification System

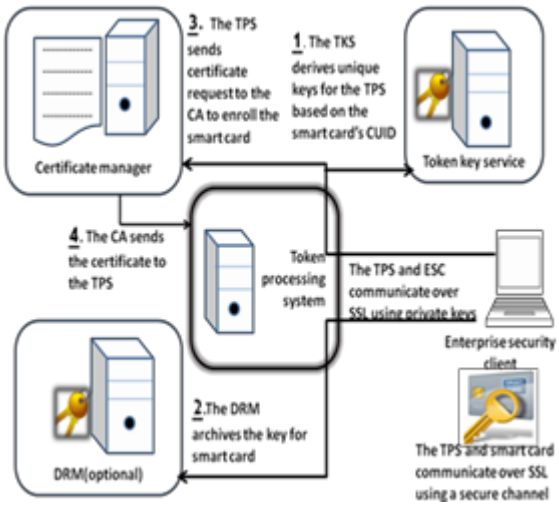


Fig. 3 Mechanism for OTP method

termed as object based. Tokens can be compared with the physical keys which are used to lock and unlock houses for security purpose that are used as a token but in digital tokens many factors are used to provide safety of information of a user. In this digital world, security tokens are used for information security. Tokens themselves have passwords so even if they are lost, the hackers cannot get the information. Bank Credit cards, smart cards are security token storage devices with pass codes and passwords. Pass code is a string of characters used as a password specially to gain access to a computer. There exist one time security tokens and smartcards as shown in Fig. 2.

1) One time security tokens:

Leonard Adleman, Ron Rivest and Adi Shamir (RSA) algorithm uses one time security token, that is, secureID. The risk is reduced by secureID as compared to a simple password. We change our passwords according to our mind in every 30 to 60 days or may be longer. But secureID works differently, it changes password in every 60 seconds, which is produced by some mathematical algos and only known to the security server. As user logs on to network of his company, he enters userID and some numbers displayed on the screen. By encryption technique this information is sent to the security server. So user will be authenticated only when the number matches the mathematical algorithm and the ID that displayed on the screen during login. Combination of userID known to the user and OTP makes this authentication so much stronger. Fig 3 shows the sequence of events that occur during the process of OTP.

C. Biometric Based Authentication:

Biometric authentication is a process to verify that a user is whom he is claiming to be, using digitized biological signature of that user. Biometric based authentication can be classified into two types: behavioral and physiological.

1. Behavioral Authentication - In the case of behavioral authentication voice prints, signatures and keystrokes are used.
2. Physiological Authentication - In physiological authentication faces, finger prints, hands, iris and retina are used.

This technique can be termed as ID based. This technique is more secure as compared to token and password based authentication techniques. Biometric authentication technique is currently in operation in various enterprises.

Table II
Comparison of commonly used Biometric Authentication Techniques

Technology Characteristics	**Facial**	**Hand**	**Iris**	**Finger Print**
Work	Capture pattern	Measures structure of hand and compare it	Capture pattern of iris and compare it	Capture fingerprint pattern
Effect with	Variable	Constant	Constant	Constant
Performance	Low	Medium	High	High
Performance affected by	Lighting	Hand injuries	Poor eyesight	Dry
Device cost	Moderate	Moderate	High	Low

IV. AUTHENTICATION TECHNIQUES'S PARAMETER'S STRENGTH'S COMPARISON

To compare the above three authentication techniques, we consider three important factors shown in the Graph I and calculate the farraginous of all those factors to determine the binding strength which will become the single point of comparison.

But, the model that is used to find out this comparative value makes use of individual weakness rather than individual strength where weakness = 1/strength. The following equation is got as a result of this comparison:

Binding Weakness = Procedural Weakness + Technical Weakness + Discriminatory Weakness

By setting up the above equation, we will find out the individual strengths as per the following parameters:

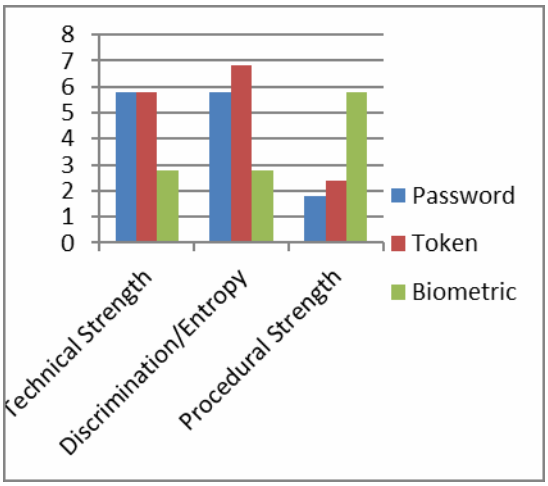
1. Discrimination Strength: For passwords, numbers of attempts are allowed in a defined time period. In case of

tokens, we consider their distinct numbers. Whereas, for Biometrics, we have a need to find out the number of different attempts are feasible.

2. Technical Strength: For all above three authentication techniques, security evaluation process is carried out.

3. Procedural Strength: It is hard to determine the procedural strength as it depends on some environmental factors such as website security and staff discipline. But, still we use a specific set of parameters to quantify the values such as randomness, length and frequency of change in case of Passwords; user discipline and physical security in the case of Tokens and for Biometrics mechanism, inherent strength is sufficient.

Next, we use these values into the above equation and determine the Binding Strength for each authentication technique.



Graph I Comparison of authentication technique's parameter's strength

After analyzing the Table III and Graph I, it can be summarized that technology characteristics of the three different authentication techniques including their hardware requirement, ease of operation, running cost, initial setup cost and vulnerability to attacks such as DOS (Denial-of-Service), technical strength and procedural strength. Password based authentication technique provides hashing and high key space which protects from host attacks. It is a convenient and inexpensive technique. Token based authentication technique is significantly more robust against attacks because of twin password combination.

In comparison to above two authentication techniques, biometric technique cannot be easily hacked so it provides stronger security but it is more expensive for personal use. So according to use the authentication techniques can be chooses by people as per their need, cost and sensitivity of data available, because no one method can be suggested as per the analysis.

Table III
Summarization of three authentication techniques

Technology Characteristics	**Password Based**	**Token Based**	**Biometric Based**
Easiness of operation	simple	simple	simple
Hardware used	No need of	Require smart card	No need of
Initial cost	Moderate as it requires simple computers	Moderate because only smart cards are required	High as it requires specialized hardware
Running cost	Expenses on system maintenance	Expenses on card maintenance	Expense of maintaining special hardware
Changes	Changed as per user's requirement	Can be changed	Never changed
Client attacks	By Guessing the password by trial	Exhaustive search	False match
Host attacks	Plain text theft	Pin code can be stolen	Template can be stolen
Denial of Service (DOS)	By multiple failed authentication Lockout	Lockout	Lockout

V. MULTIFACTOR AUTHENTICATION

To make network more secure, a combination of above authentication techniques need to be used as shown in Table 4. This is defined as multi-factor authentication. For security of network, each authenticator's result must be satisfied. AND operation is used for each factor's authentication results, so all must be assertive. In ATM cards two factor authentications are used the card itself and its password. So even if the card was stolen or lost, we can be sure that the safety is maintained until hackers don't know password. This is an example of password plus token based are mostly implemented in this time. Other combinations of token and biometric authentication are also considered as secure techniques if it's difficult for a user to memorize passwords, but they need costly machines.

But the combinations of biometric and passwords authentication are not so common because biometric usually consists sake for convenience. Combination of all three factors is needed where there is a high security is required. Till now this type of combination is not highly applied. Combinations of these three authentication technique are shown in Table IV.

Table IV
Combination of different Authentication Techniques for better Security

Authenticator Combination	**Password -Token Based**	**Password-Biometric Based**	**Token-biometric based**	**Password-Token-Biometric Based**
Security	Good	Better	Better	Best
Cost	Moderate	High	High	High
Advantage	Lost token is Secured but protected by password	Biometric provide security if password is forgotten	Lost token is secure but protected by Biometric	Three factors provide add on security
Drawback	Memorize password and always carry tokens	Memorize password and have Biometric ID	Always have to carry ID but not if it is a Biometric	Have to memorize password, have Biometric ID and carry Token
Real life example	ATM cards	Password Biometric for any Access	Photo ID proof	Where high security requires like MILITARY

CONCLUSION

Network security can be maintained by using various authentication techniques. User has to use authentication technique according to requirement. Password based technique is best if you are able to memorize a single password. But problems occur when we try to memorize many passwords so we use those passwords that are easy to memorize. Token based authentication techniques procure additional security against DOS (denial of service) attacks. In comparison to the above two authentication techniques biometric cannot be easily hacked so it provides stronger security. As signals, biometric can be easily duplicated by hackers so it should not be deployed in single factor mode. Furthermore we can select a combination of above three techniques as discussed above. All authentication techniques have their advantages and disadvantages. We have to be smart to choose techniques as per our necessity of safety of networks and information by considering cost factoralso.

REFERENCE

[1] Password based Authentication Techniques: https://technet.microsoft.com/en-us/library/cc732393(v=ws.10).aspx
[2] Biometric based Authentication Techniques: http://www.computerworld.com/article/2556908/security0/biometric-authentication.html
[3] L O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Vol. 91, Dec. 2003 at IEEE,
[4] Hafiz Zahid Ullah Khan, "Comparative Study of Authentication Techniques", IJVIPNS Volume - 10.
[5] J J Kim and S P Hong, "A Method of Risk Assessment for Multi-Factor Authentication", JIPS, Vol.7, in 2011.
[6] Q Li, Student Member of IEEE, and G Cao, Fellow of IEEE "Multicast Authentication in the Smart Grid with One Time Signature", VOL. 2, December 2011, IEEE.
[7] Advance Authentication Techniques: http://ids.nic.in/technical_letter/TNL_JCES_JUL_2013/Advance%20Authentication%20Technique.pdf
[8] Stamati Gkarafli, Anastasios A. Economides, "Comparing the Proof by Knowledge Authentication Techniques", Volume 4, IJCSS.
[9] Roger Meyer, "Secure authentication on the internet", SANS 2007.
[10] R. Morris, K. Thompson, "Password security: A case history", Vol.22, pp. 594-597, Nov. 1979.