International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 5, Issue 05, May-2019

A survey on various existing Authentication Mechanisms and their comparison based on Security Criticality and Computational Cost

Mitul Patel

School of Engineering, P P Savani University, Surat,

***Abstract*— In the current world of technology, when billions of information is being transmitted from one corner of world to another corner, security is an important aspect for protection of those information from any unauthorized users. The three security issues important to provide restriction to unauthorized access are: identification, authentication and authorization. Identification is a process to prove user's identity like username. Authentication is a process to verify user's identity. Authorization is a process to provide access to various resources after identification and authentication. In this paper I have reviewed various existing authentication methods and also compared them based on various factors like security criticality, computational cost, advantages, disadvantage and applications of each.**

***Keywords—* Authentication, multifactor authentication, certificate, NTLM, Kerberos, zero knowledge, CAPTCHA**

INTRODUCTION

In Today's digital world where information is being transmitted in a fraction of second, it is very much important to include the concept of cyber security with each and every transaction. Cyber security means protecting your information from any type of disclosure, disrupt or modification. In short to be secure, information should be hidden from unauthorized access (confidentiality), information should not be changed by unauthorized person (integrity) and information should be available to the authorized user whenever he wants (availability)[1][2]. There are many technologies are there and still so much research going on for security of information, still there are many malicious activities performed by some unauthorized user that will compromise the confidentiality and integrity of information.

The International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) has provided some security services and some security mechanism to implement those security services. The security services defined by ITU-T are as follows [1]:

- ***Data Confidentiality*** – protecting data from unauthorized disclosure
- ***Data Integrity***-protecting data from unauthorized modification
- ***Authentication***- authentication (proof of origin/entity authentication) of sender or receiver
- ***Non-repudiation*** – protection against repudiation of sender or receiver
- ***Access Control*** – protection against unauthorized access to data

There are many techniques are there for implementation of each security services [3], but in this paper I have majorly focused on authentication. This paper is organized in four sections. In section 2, I have defined the authentication and basic steps involved in authentication process. In section 3, I have reviewed various authentication methods available in existing system and in section 4; I have performed the comparative analysis of various authentication methods based on the various factors like security criticality, computational cost, advantages, disadvantages and applications of each.

I. AUTHENTICATION DEFINITION AND STEPS

Authentication means to check whether the user at other side (sender/receiver) is authenticated user (having rights to send or receive data) or not. Authentication technology basically checks the user's identification with the stored identification in database to check whether there is matching or not. If matching is found, user is authenticated otherwise the user is not authenticated and he will be not given any access to use further information. The simplest example of user authentication is password-based authentication. When the user registers with any web-site or any organization, he has to prove his unique userID and password which is stored on authentication server. When the user wants to login again, his credentials are checked with stored credentials. Only the users having matching credentials can login to system and get further information.

The 'OSI Security Architecture' has given two different meaning of authentication: Data-origin authentication and (peer) entity authentication [4].

- ***Data-origin authentication***: verifying the origin of received data. E.g. authenticating the user by Digital Certificate where electronic signature can prove the authenticity of sender [1].
- ***Entity authentication***: verifying the identity of one entity by other. An entity can be a person, a process, a client or a server. E.g. Password based authentication and biometrics [1].

There are two differences between data-origin authentication and entity authentication.

1. Data-origin authentication might not happen in real time but entity authentication always happens in real time that means when sender sends a message to receiver and when receiver verify it, the sender may or may not present in communication but in case of entity authentication, first sender is authenticated by receiver then only he can communicate with receiver. Data-origin authentication requires when sender sends an email to receiver. Entity authentication requires when a person withdraw money from ATM.
2. Data-origin authentication need to be repeated for each new message (different certificate for different message) while entity authentication authenticates the sender for the entire duration of a session. (Single log-in for online banking).

An authentication factor represents some piece of data or attribute that can be used to authenticate a user requesting access to a system. In entity-authentication, the receiver can verify the sender based on three authentication factors:[5]

- ***Something known***: some secret or credentials known to only sender like password, PIN, secret key or a private key.
- ***Something possessed:*** something that can prove the sender's identity like a passport, a driving license, Aadhar card or a pan card.
- ***Something inherent***: some inherent characteristics of the sender like conventional signatures, fingerprints, voice, facial characteristics, retinal pattern and handwriting.

A SURVEY ON EXISTING AUTHENTICATION MECHANSIMS

Traditional authentication depends on security of password-based file where userID is stored along with hashes of password for each registered user. When the user wants to login the system, the user's userID and Hash value of entered password is compared with the stored values in password files. If matches found, the user is authenticated. This approach to authentication has various draw-backs like the attacker who is able to access the password file can use brute-force attack to extract password. Also, it requires multiple authentications for accessing resources on multiple systems.

Here I have listed some authentication methods currently being used for various application and tried to compare with each-other. Various authentication methods are as follows:

A. HTML forms-based authentication[6]

The simplest authentication scheme and majorly used authentication scheme is HTML forms-based authentication where the user who wants to use the system is provided with login form where he has to enter his credential details. It can be classified into two sub categories:

- ***Password based*** [7]: User has to enter userID and password which are checked against stored userID and password. If matched found, the user is authenticated. It's least secure scheme. Some of the attacks possible on this authentication scheme are password stolen attack (replay attack), brute-force attack and also some physical attacks like camera recording a PIN. One of the solutions to increase the strength of password is to perform Hashing of password but a stolen password hash could sometimes be reverted, for example, by using a list of precomputed hashes of the most common passwords or more sophisticated attacks like using rainbows-tables;
- ***SMS based on One Time Password*** [8]: The replay attack on password-based scheme can be overcome by use of OTP by generating a new password for each new user. There is some specific hardware or some software routine to generate OTP for each new user. The OTP is sent to the mobile-phone or email-id. Once user enters OTP along with user-id then only he will be able to login to system. This scheme is secure against replay attack but it requires the security of channel through which OTP is sent to the user.

B. Multifactor mechanisms, such as those combining passwords and physical tokens.[9]

In multifactor authentication, user is authenticated by more than one factor. It can be accomplished through biometric factors like fingerprint, iris, voice or some possession factors like security keys. There are basically three types of authentication factors used in multifactor authentication [10].

1) ***Knowledge:*** Something that the user knows e.g. password and PIN. There are two kinds of knowledge-based authentication: Static KBA and Dynamic KBA. In static KBA, users have to set answers of some security questions when they set up a system or password-protected profile. If the password is forgotten or the user wants to renew the password, he has to provide the answers to security questions that he has provide earlier. In dynamic KBA,[11] the user will be provided such type of security questions whose answers are known to user as well as the system. The IT systems know the answer by performing some data mining technique on previously gathered data of the user. Although the security criticality of dynamic KBA is high, many companies prefer static KBA due to the challenges involved in dynamic KBA.
2) ***Possession:*** Something the user has e.g. hardware token. Users are authenticated by some devices or objects like smartcards and Universal Serial Bus (USB) [12].The tokens (devices) used in possession-based authentication can be connected tokens or disconnected tokens. Connected tokens can be card readers, wireless tags or USB tokens while a disconnected token [13] device will use a built-in screen to display authentication data which is then utilised by the user to sign in, where and when prompted.

3) ***Inherence***: Something that verifies the user e.g. Fingerprint or voice. Inherence factor are biometric factors of users [14][15]. The user is authenticated based on some physiological characteristics like fingerprint, iris movement or voice or user is authenticated based on some behavioural characteristics. Some distinguish and repeatable features can be extracted from the user for the purpose of automated identification.

In this paper I have analysed various knowledge-based factors (static and dynamic), possession-based factors (connected token vs disconnected tokens) and inherence factors (fingerprint reader, iris scanner and voice). I have compared all of them based on the security criticality, computational cost, advantages and disadvantages of each (**Table II**)

C. Client SSL certificates and/or smartcards [17]

In this authentication technique Digital Certificates are used to identify a user before granting access to any resource or web-site. Using the Digital Signature, the sender can electronically sign the data and verifier can electronically verify the signature. This technique involves a private-public key pair where sender can sign the data using his own private key and receiver can verify the signature using sender's public key. Due to the user friendliness, easy of deployment and ongoing management and high security, it is widely used authentication technique in current market. The problem associated with this technique is cost of generation and distribution of digital certificates.

D. HTTP(Hyper Text Transfer Protocol) basic and digest authentication[18][19]

In HTTP basic authentication when client wants to access some protected resource at server side, the server will ask client to send some authentication credentials like username and password. In response, the client will send username and password to the server in plain text on secure SSL layer. The server will check the credentials sent by the client with the values already stored in database, if matched found, the sever responds with the desired information.Basic Authentication uses base64 encoding for generating cryptographic string which contains the information of username and password.

HTTP digest authenticate is same as basic authentication but here the client will send credentials in an encrypted form by applying a hash function to the username, password, a nonce supplied by server, the HTTP method and requested URI. So, I can say that digest authentication is more secure than basic authentication.

E. Windows-integrated authentication using NTLM or Kerberos [20]

Widows-integrated authentication using NTLM (NT Lan Manager) is used for those users which are using Microsoft Windows NT based operating systems. When the user who is authenticated by windows during login sends a request to access protected page of a windows application, the server will reject the request and sends a response saying user to be authenticated using NTLM. The client browser gets the user's windows login credentials, performs the hash and sends to the server. If the hashes match at server side, the server creates a unique and encrypted challenge to send back to client which can be decrypted by the user's password only. The client decrypts the challenge and send back to server. The server checks the response. If the answer is correct, the user is authenticated and the protected resource is granted otherwise it will send unauthorized message to the user.

The problem with NTLM authentication is that the client needs to be authenticated every time if he wants to access pages from different servers. Kerberos based authentication uses three different servers naming AS (Authentication Server), TGS (Ticket Granting Server) and Real Server. Once client is authenticated by AS, he can communicate to any real server for accessing different pages.

F. Authentication services

The two most widely use authentication services are: zero knowledge proof [21] and CAPTCHA [22]. The zero-knowledge proof authentication allows a party to prove that he knows the credentials without having transmission of those credentials. With ZKP there is no transmission or storage of credential details on the authentication sever. CAPTCHA is an authentication process based on challenge-response authentication where user can protect them for spam and password decryption by taking a simple test. In this test, user will see either a text or an image in distorted form or sometimes user is asked to solve some mathematical equation. If the user is able to enter correct text or able to solve the equation, the user is authenticated otherwise the user is unauthenticated. CAPTCHA is also used in the sites which provide access to sensitive data such as credit card accounts and bank. The CAPTCHA can be text based, image based, voice based or sometimes video based.

COMPARATIVE STUDY

In this section, I have tried to compare various authentication methods that we have studied in section III(form-based authentication, multifactor authentication, Certificate based authentication, message digest-based authentication, integrated authenticated and various authentication service) based on various factors like security criticality, computational cost, advantage, disadvantages and current use in real time systems. The comparisons are shown in
Table I .

Multifactor authentication includes three major authentication factors like knowledge based, possessions based and inherence factors. I have also tried to compare those factors based on the security, cost, advantages and disadvantages. The comparisons are shown in **Table II.**

TABLE I
COMPARATIVE ANALYSIS OF VARIOUS AUTHENTICATION MECHANISIMS

Types of Authentication		**Security Criticality**	**Computational Cost**	**Advantages**	**Disadvantages**	**Applications**
Form based Authentication	Password based	Low	Low	Simple to use, Simple to deploy	Security completely depend on confidentiality and strength of password, No protection against replay attack	Email account, Social Networking website
	SMS based on One Time Password	High	High	Easy to use, Secure again replay attack	Extra cost of OTP generation, security of channel through OTP is shared	Password Recovery, Banking, Online payment
Multifactor Authentication		TABLE II				Industrial organization, ATM access etc.
Certificate based authentication (SSL Authentication)		High	High	Giving a Trust to visitor, easy Verification by visitor. Gives integrity of Data.	Cost of certificate generation, Problem with existing files having HTTP, additional cost for proxy caching and in-house software set up.	All HTTTPS (Hypertext Transfer Protocol over Secure Socket Layer) web-sites.
HTTP basic and digest Authentication		Low	Low	protection for Replay attacks, Mutual authentication and Integrity protection	Susceptibility of algorithm against pre-image, second pre-image and collision resistance attack	Online banking, Mobile Cloud Computing
Integrated Authentication	Windows Integrated Authentication Service using NTLM	High	High	easy to configure and no additional configuration to function correctly	requires multiple exchanges between the client and server, connection break create problem	All windows NT based operating systems.
	Windows Integrated Authentication Service using Kerberos	High	High	Faster than NTLM and allows the use of mutual authentication and delegation of credentials to remote machines, open protocol	Requires additional configuration to function correctly, Requires client have connectivity to KDC	Windows 2000, Windows XP and later all windows operating systems
Authentication Services	Zero Knowledge proof	Low	Low	No revelation of secret, No complex encryption methods	Extra processing for text secret, slow computation, Interception is possible	Online Voting, Privacy on public block chains
	CAPTCHA	Low	Low	Limit spam, easy to implement	Distorting text and pictures, prevention of spam not possible	Most major web-sites, online trading, online game authentication etc.

TABLE II
COMPARATIVE ANALYSIS OF VARIOUS AUTHENTICATION FACTORS OF MUTIFACTOR AUTHENTICATION

	Multifactor Authentication								
[16]	**Knowledge (Something user know)**		**Possessions (Something user has)**				**Inherence (Something user is) (Biometric)**		
	Static Scheme	**Dynamic Scheme**	**Connected Tokens**			**Disconnected Tokens**	**Fingerprint readers**	**Iris Scanners**	**Voice**
			Card Readers	**Wireless tags**	**USB tokens**				
Security Criticality	Low	High	High	Low	High	High	High	High	Low
Computational Cost	Low	High	High	High	High	Low	Low	High	High
Advantages	Pre-agreed Questions and answers, easy to set up	able to prevent fraud and offer customers added protection	More secure than Payment cards and adaptable to system	No need of LOS, Easy to deploy in Real time Applications	Third Part Authentication Increase trust	Simple to Use, immune to coverage, latency, and delivery issues, Supports data Signing function	Economic and easy	Most accurate, one sample can last for lifetime	Reliable Easy to use
Disadvantages	Attacker can Use public Information of entity to find answers	difficult to implement and requires hard-to-acquire information	Installation And Distribution of certificates	Easily intercepted, Limited coverage Range	User need to carry an additional Smart card	Possibility of web attacks, breach of codes, susceptible to fraudster attack if OTP generator poorly implemented	Time taking, dry and dirty fingertips	Expensive, Susceptible To poor Image Quality	Stealing Of Voice is Possible, Require more File storage

CONCLUSIONS AND FUTURE WORK

Here I have studied six different authentication mechanisms namely HTML form based authentication, multifactor authentication, certificate based authentication, HTTP basic and digest authentication, integrated authentication and various authentication services. I have also explored the various authentication factors involved in each authentication scheme like HTML form based authentication can be either password based or OTP based, multifactor authentication can be knowledge based, possession based or inherence based(Table II) while integrated authentication can be either NTLM based or Kerberos based. I have performed the comparison of all these authentication mechanisms based on various factors (Table I).The table shows that all authentication mechanisms have its pros and cons. If we want to achieve better security with less computational cost, we can combine multiple authentication mechanisms. These techniques can also be compared with respect to their usage in various application like distributed applications, IoT applications or cloud-based applications [23][24]

As the technologies grow day by day, we can incorporate new security techniques in previous authentication techniques to achieve higher security. Also, there are many security attacks that can affect the security criticality of authentication mechanisms. So, we can compare the various authentication techniques based on the security criticality against various security attacks.

So, the final conclusion is we require a strong authentication mechanism that must be secure against various security attacks and can be implemented with least computational cost. All authentication schemes have its pros and cons so we can combine multiple authentication mechanism for better security or we need some strong authentication mechanism which satisfies the all authentication requirements of any applications.

REFERENCES

[1]. William Stalling, "*Cryptography and Network Security Principles and Practices*", Fourth Edition, Prentice Hall Publications.

[2]. Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. "*A. Handbook of Applied Cryptography*". ISBN 0-8493-8523-7.

[3]. Rima Saliba, Gilbert Babin, Peter Kropf, "*SecAdvise: A Security Mechanism Advisor*", University of Montreal.

[4]. Chris Mitchell, "*Authentication using Cryptography*", Information Security Group,8th September,1997

[5]. Syed Zulkarnain, Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Jean-Jacques Schwartzmann, "*A Review on Authentication Methods*", University Malaysia Perlis.

[6]. Rehman Ullah Khan,Waleed Albattah, "*Security and Safety Concerns: Username and Password Paradigm*", IJCSNS International Journal of Computer Science and Network Security,VOL.17 No.10,October 2017.

[7]. Shameer Mohammed, Dr.L.Ramkumar, V.R.Rajasekar, "P*assword-based Authentication in Computer Security; Why is it still there?*",The SIJ Transactions on Computer Science Engineering & its Applications (CSES),Vol.5,No.2,March 2017.

[8]. Abdulrahman Alhothaily,Chunqiang Hu,Arwa Alrawais1, Tianyi Song, Xiuzhen Cheng,Dechang Chen, "*A secure and practical authentication scheme using personal devices*", IEEE Access, Vol 5,2017,dop,June 21,2017.

[9]. Mahmoud Musa Mohammed, Dr. Muna Elsadig, "*A Multi-layer of Multi Factors Authentication Model for Online Banking Services*", International Conference on Computing, Electrical and Electronic Engineering (ICCIEEE),2013, IEEE.

[10]. Jae-Jung Kim,Seng-Phil Hong, "*A Method of Risk Assessment for Multi-Factor Authentication*" Journal of Information Processing Systems, Vol.7, No.1, March 2011 DOI : 10.3745/JIPS.2011.7.1.187

[11]. M. L. Das et al., "*A Dynamic ID-based Remote User Authentication Scheme*", IEEE Transactions on Consumer 630 Electronics, Vol. 50, No. 2, MAY 2004.

[12]. Jiang Yu, Chuan-fu Zhang, "*Design and Analysis of a USB-Key based Strong Password Authentication Scheme*"

[13]. Steffen Hallsteinsen, Ivar Jørstad, Do Van Thanh, "*Using the mobile phone as a security token for unified Authentication*", Second International Conference on Systems and Networks Communications (ICSNC 2007).

[14]. Kresimir Delac, Mislav Grgic, "*A Survey of Biometric Recognition Methods*", 46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June 2004, Zadar, Croatia

[15]. "*Biometric Recognition: Security and Privacy Concerns*", IEEE SECURITY & PRIVACY, MARCH/APRIL 2003

[16]. Lawrence O'Gorman, "*Comparing Passwords, Tokens, and Biometrics for User Authentication*", Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040 ã 2003 IEEE.

[17]. Manik Lal Das,Navkar Samdaria, "*On the security of SSL/TLS-enabled applications*",, Elsevier B.V., 26th February 2014.

[18]. J.Franks et.al. "*HTTP Authentication: Basic and Digest Access Authentication*", the internet Society (1999).

[19]. Aruna S. "*Security in Web Services – Issues and Challenges*", IJERT, ISSN: 2278-0181, Vol. 5 Issue 09, September-2016

[20]. Randhir Bhandari,Sachin Sharma,Nagesh Kumar, "*Analysis of Windows Authentication Protocols: NTLM and Kerberos*",ResearchGate Conference,DOI:10.13140/2.1.2057.5528,March 2014

[21]. Wang Huqing,Sun Zhixin, "*Research on zero-knowledge proof protocol*", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013

[22]. A.B. Jeng et al., "*A Study of CAPTCHA and Its Application to User Authentication*", J.-S. Pan, S.-M. Chen, and N.T. Nguyen (Eds.): ICCCI 2010, Part II, LNAI 6422, pp. 433–440, 2010.

[23]. Jesudoss A. et.al, "*A Survey on Authentication Attacks and Countermeasures in a Distributed Environment*", ISSN : 0976-5166 Vol. 5 No.2 Apr-May 2014

[24]. Marcos A. Simplicio Jr. et.al. "*Comparison of Authenticated-Encryption Schemes in Wireless Sensor Networks*", 36th Annual IEEE Conference on Local Computer Networks

[25]. Maha M. Althobaiti, Pam Mayhew, "*Usable Security of Authentication Process:New Approach and Practical Assessment*", The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015)