ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
June 2017,
Vol. 10, No. (2):
Pgs. 513-519

A Survey on User Authentication Techniques

K. SHARMILA[1*], V. JANAKI[2] and A. NAGARAJU[3]

[1]*Department of CSE, Aurora's Research and Technological Institute, Warangal, Telangana, India*
[2]Department of CSE, Vaagdevi College of Engineering, Warangal, Telangana, India
[3]Department of CSE, Central University of Rajasthan, Rajasthan, India
*Corresponding author E-mail: sharmilakreddy@gmail.com

http://dx.doi.org/10.13005/ojcst/10.02.37

(Received: May 02, 2017; Accepted: May 20, 2017)

ABSTRACT

Confidentiality and Authentication were once treated different but now-a-days, improvement in technology is demanding both of them to be used together. Though technology is increasing tremendously, smart hackers on the environment always challenges the authentication factors, thereby enforcing more number of factors for authentication to be included. As factors increase, failure rate for authentication may also be more when any one of the factors doesn't work. A qualitative survey of user authentication systems being used in today's environment is presented here and a comparative study of various authentication mechanisms used in the world of Information security by various researchers is shown.

Keywords authentication, cryptography, smart cards, social authentication, tokens, vouching.

INTRODUCTION

Cryptography is the art of providing security for information and resources by implementing suitable technologies. In Information security, cryptography plays a vital role in achieving confidentiality, integrity, authentication and non-repudiation. Identification and authentication of a user to the system is equally important as privacy in our lives. Increase in usage of electronic communication, needs to have electronic techniques for providing authentication. Cryptography is a system built for providing secure communication of data, identification of user, authenticating the user based on valid credentials. Complicated applications such as digital certification, secure e-mail transmission, key recovery etc are also addressed by cryptography. Identification and authentication are the two extensively used applications of cryptography. Identification is the process of recognizing a user and authentication determines whether the user is authorized for performing the action.

Related work

Passwords are very commonly used factors of authentication. But they are prone to guessable attacks[1]. To overcome these attacks, the passwords have to be changed frequently. If the user cannot recollect his/her password, knowledge-based authentication systems are helpful to regain another password with the help of their e-mail or registered mobile number[2]. Security questions also can be implemented where a unique question related to the user like his first school name or mother maidens name is posed by the system, which can be answered only by the original user. This helps the user to regain access to the system temporarily[1].

To overcome the disadvantages of passwords, Smart cards have come in to existence. Smart cards are devices externally made of plastic with an embedded integrated computer chip[3,4]. It can store data of 64KB and can be read by a terminal called smart card reader. Security mechanisms are implemented to secure the information stored on the smart card[3,5]. Smart cards enable a strong authorization, confidentiality, security and integrity to the users. If the user possesses a card, he has to use it along with a key or PIN[4,6]. Electronic keys and smart cards in combination are mostly used for accessing in to workplaces and to withdraw money from ATM machines. If the user forgets the PIN or if the card gets stolen or lost, authentication may not be possible[7].

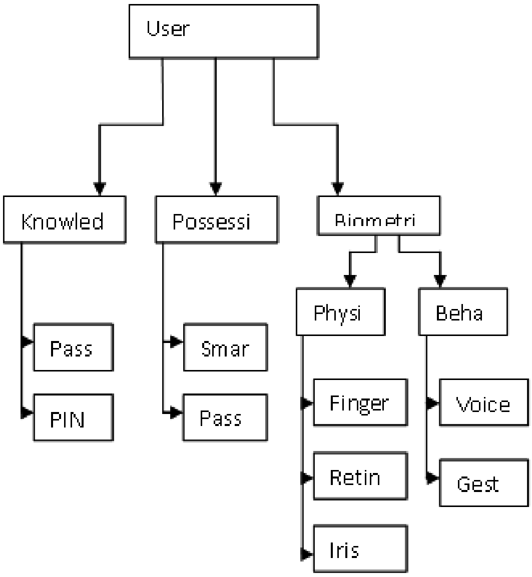

Fig. 1: Existing user authentication techniques

The flaws of one factor and two factor authentication techniques are overcome by the implementation of biometrics[8]. Identifying a person based on his physical characteristics has become a widely used factor of authentication. As no user has identical signs of physiological characters with the other, this is considered as unique factor of authentication. The system will compare the physical characteristics like a fingerprint, handprint, retina pattern, Iris and voice with the values already stored in the database and determine whether the user is authentic or not. The biometric system sometimes may reject even a valid user. These systems are not widely implemented because of their maintenance cost. In the following sections, we discuss about the survey made on different kinds of authentication factors proposed by various authors.

One factor authentication

The most common authentication mechanism is in the form of passwords. Users tend to remember them, note them down and use them. A study was conducted by the authors Vu et al. in 2007 on password memorability[5]. As part of the study, 12.5% of the users forgot their registered six-character passwords after one week. A survey conducted by SafeNet revealed that 47% of users forgot their passwords and they had to be reset timely[5]. Often, password mismatches do occur when users mistype their passwords or get confused to use one password out of their multiple passwords. Brostoff and Sasse observed that giving more chances to the user, while entering a password would definitely reduce password reset requests[7].

A Survey of user authentication mechanisms by Magno, Marianna B

Accessing a computer system requires a computer security manager and system administrator to monitor authorized users, unauthorized users and various operations of the systems[10]. This can be done by the two step process using identification and authentication. In order to make certain that only a correct user can access a system, the user has to authenticate himself by providing valid user name and valid password. There are many systems existing for authentication using passwords, smartcards and any of the biometrics but they are prone to attacks and are less secure.

Anyone can log in to the system by providing the authentication factors[10]. There are several methods for user authentication[3]. The three most commonly used methods are shown in fig. 1.

1. Knowledge based-Something You Know
2. Possession based-Something You Have
3. Biometric based-Something You Are

Identification and Authentication: Technology and Implementation Issues by M. Zviran and Z. Erlich

The authors have described about different types of passwords. They have concentrated on cognitive passwords, where the user need not memorize the password but he knows it and can recollect it, whenever required. While using this cognitive password system, the user provides answers to personal fact-based or opinion-based questions, posed by the system[2], like the user's first school name (fact-based) or user's hobbies (opinion-based). Because cognitive password system is easier to use when compared to conventional passwords, it is suggested as a better way to defeat the difficulty of remembering passwords.

Two Factor Authentication

Two Factor Authentication Using Mobile Phones by Fadi Aloul, Syed Zahidi, Wassim El-Hajj

Fadi Aloul[7] has described a method of implementing two factor authentication using mobile phones instead of using software tokens or smart cards. Mobile phone is used to generate one time password, which can be further used as a token. OTP generation was implemented and tested in real time environments. The authors have proposed a mobile based software token system which can be used to replace the usage of hardware and software tokens together. This system consisted three parts, a software in the client's mobile, a software at the server side and internet facility so as to connect to the server. This could be operated in two modes. Connection less mode and SMS based authentication mode. In connectionless authentication system, the mobile phone acts as a token and uses unique factors to generate an OTP locally. The server has necessary factors along with the unique values corresponding to each mobile phone to generate the password. The server, then compares the value with the password submitted by the client. In SMS based authentication system, the mobile phone can get OTP from the server directly. For the server to verify the identity of the user, the user sends his unique information in the form of a SMS. The server verifies this message and if found true, sends an OTP to the user's mobile phone[11].

A New Two-Server Approach for Authentication with Short Secrets by John Brainard, Ari Juels, Burt Kaliski, and Michael Szydlo, RSA Laboratories.

John Brainard, et.al[4] has proposed basic security problems that can occur over internet while authentication. They have designed two server roaming system where a user splits his/her password in to two parts in a random manner. The server then compares these two shares using a protocol without leaking any additional information. By implementing two servers, this system provides more security to the sensitive user data when compared to single server approach. Some of the attacks that are possible on the internet like replay attacks, false-pseudonym attacks could be overcome by this proposal.

Two-factor mutual authentication based on Smartcard and passwords by Yang, G Wong, D. S Wang, & Deng X.

Yang et al. have proposed a technique[11], where a plug-n-play device is used to provide input. This requires username, password and smart card authentication for providing confidentiality. The smart card responds with the corresponding verification value and hence the user is given a chance to access the files. The advantage of this method is that it protects from forgery attack, as the device id is recorded. The two-factor authentication[12] based on smart cards, should own the smart card to certify the passwords. This kind of authentication provides stronger security when compared to normal password based authentication. Nevertheless, this method also can be challenging if the two factors are compromised i.e there is every chance for the attacker to acquire the data stored in the smart card along with the password.

The authors[11] have developed a two factor control protocol based on mutual authentication and key agreement. In their proposal, both the storage device and correct password have to be submitted simultaneously to make a successful authentication.

Three Factor Authentication

A Global look at authentication, stephen s. Hamilton, martin c. Carlisle, and john a. Hamilton jr

Stephen S et.al[6] proposed how authentication is provided for the users using their unique identity like passwords, smart cards and then biometrics. In all the authentication schemes, except biometric, there exists recovery problem when an authentication token is lost. The general form of recovery used is posing some questions which are unique and provided by the user at the time of registration or sending a password reset link to the user's email address. The security question concept may not work well because anyone can have minimum knowledge of common things such as favorite colors, pets and first teacher. The other common way of sending the password through email works, may not be implemented securely. As email is sent in the form of readable text, the password may be compromised. Biometrics are secure but their implementation may be costly[13]. Centralized authentication system procedures, centralized password storage and recovery methods are also learnt. As technology is increasing, identity theft is also growing and therefore the users have to be very cautious.

Multifactor Authentication Systems by Jiøí Sobotka, Radek Doležel

Jiri Sobotka, Radek Dolze[6] described one factor, two factor and three factor authentication techniques and their applications. They have proposed building of Security infrastructure with hardware and software tokens and secure connection could be established through HTTPS with tokens. Two versions of generating emergency token code, a temporary fixed token code, a set of one time token codes were utilized. In their infrastructure, applications that represent the Open Source Software projects were used. On the client side, the applications that support operating system for working with tokens is involved in Application layer. HTTPS is used for communication. A base of this protocol is SSL/TLS that operates on lower layers. For successful connection establishment, a web server on the server application and a web browser on the client application are used. The web server used is Apache HTTP Server and the web browser can be any standard web browser compatible with certificates and tokens.

Four Factor Authentication

Fourth Factor Authentication: Somebody You Know by John Brainard, Ari Juels, Ronald L. Rivest, Michael Szydlo, Moti Yung

Brainard et.al[3] proposed Fourth Factor Authentication where the authors have designed a mechanism beyond existing authentication techniques like one factor authentication, two factor and three factor authentication techniques. They have addressed the advantages and disadvantages of all the three factors of authentication. The types of tokens like Hardware tokens and software tokens were discussed. The authors have proposed a protocol based on social relationships among the humans. As trust in human relations has been used since the evolution of mankind, this relation called trust is considered as main factor of authentication. The advantage of this protocol is that emergency authentication could be provided based on social relationships in the absence of any of the existing authentication factors. However, the disadvantage is that social engineering and user behaviour cannot be predicted always.

In their work, the authors have described a vouching system for hardware authentication like RSA SecureID. A SecurID token generates a new value every sixty seconds. This value is called as called a token-code. The user has to present this token-code along with a PIN or password[4,8,10]. The token-codes are validated by an authentication server which shares a value corresponding to every generated token and PIN of the user. The normal two factor authentication protocol does not use the concept of vouching, but only demonstrates how a vouching system can be implemented. In this procedure, each user is given a PIN value and hardware token. When both are submitted together at any instance of time, a code is generated. At the server side, the user identifier is associated with its chosen PIN and the generated token-code. As a result, it produces the resultant values and compares with the values given by the user. If both the values are same then the server allows the user to continue the transaction or else it rejects the permission. Security measures have been initiated by the authors in the form of transaction logs maintained at the server that can be accessible any time.

It's not what you know, but who you know: a social approach to last-resort authentication by Stuart Schechter, Serge Egelman, Robert W. Reeder.

The authors[8] have designed a new backup authentication mechanism and studied its performance by implementing it as part of Windows Live ID. This mechanism involves social authentication, in which the account holder (user) of any bank choose helpers or trustees who can help them in the process of authentication in emergency. In this process, the users contact their helpers over telephone or personally, so that their helpers can easily recognize them by their physique or by voice. A trustee after recognizing the account holder may provide an account recovery code or OTP, which will be presented to the system to authenticate. The authors[16] believe that the success of this mechanism depends on infrastructure, maintenance cost, efficiency, reliability and security. The concept of trustee based authentication is not a new one[3]. In some organizations, the responsibility to help a user who fails to be authenticated is taken care by system administrators or help desk. Microsoft also employs trustee based account recovery mechanism for its company employees. Brainard et al. of RSA has proposed a two factor primary authentication system , where a user who lost his/her token can take the help from a pre registered trustee called as helper[3]. In this system, the helper generates a vouch- code that acts as an emergency token. But, the practical results have not been declared.

Social Authentication Protocol for Mobile Phones Bijan Soleymani and Muthucumaru Maheswaran

Using social network as authentication factor is the current trend of authentication. As part of this, the behavior of the user in his social network is studied and understood. Using these details for user authentication is under research[7]. This mechanism is not only considered as an extension to the techniques existing in the market but, it is also considered as a new approach to authentication. The authors have proposed two different ways in which this can be implemented. In the first way, the user contacts the members of his social network to authenticate him. The second way involves using the user's account details on a social networking site to contact the other members of the social network. The first approach is the one proposed in the RSA paper[7]. Here, the user contacts a friend (Helper) when he has forgotten his token. The helper logs in to the website with his/her own token, requests a vouch code on behalf of the user. This vouch code is forwarded to the user, who can use it to log in to the system once. The approach proposed by the authors[11] also falls under this category. Here, the user obtains a vouch code from his/her helpers after a telephonic conversation or any other means of communication and these tokens are used to log in. In the second approach, the user contacts his friends over the social networking websites. As these websites provide peer discovery of information and enable secure messaging, it is possible to set up a secure communication channel between user and helper so that a key can be shared via the social network. This key can be used to encrypt the transmissions that pass through the Internet. This process can be done either manually by the user, or by the application residing in the system.

Exploiting Human Factors in User Authentication by Payas Gupta

Humans, as authenticating factor is considered as one of the challenging factors of a security system, as users are described as the weakest link in the security chain [18]. In his work, the author has focused primarily on two problems caused by human factors in authentication.

Secrecy information inference attack: In this, publicly available information is used to get secret information about the user. Coercion attack: In this, an attacker forces a user to handover his/her secret information like username and password. The author focused on human vulnerability to coercion attacks. Most authentication mechanisms today are vulnerable to coercion attacks. The author[12] has presented a technique in generating cryptographic keys to overcome coercion attacks and has incorporated a measure to calculate user's emotional status using skin conductance for key generation process.

Cryptographic key is generated using lookup table method[4,16,17]. The author has carried out two experiments as part of his study and has shown interesting results. The model proposed by the author was tested with user's voice and skin conductance data. The false acceptance and false rejection rates were computed. Some results revealed that cryptographic keys that are generated in two different scenarios were different for the same person. As skin conductance and voice were not static biometrics and they could change as per some climatic or physical conditions, the results were of high false rejections in some cases.

Addressing Insider Threat using "Where You Are" as Fourth Factor Authentication by Sung Choi and David Zage.

The author proposed that authentication for any computing comprised of two parts, identification and verification. Conventionally, login IDs are used for identification and passwords for verification. Many techniques have been suggested by various researchers to improve the traditional techniques. But some of them required specialized devices or they were not much reliable. The authors Sung and David[17] have proposed a scheme that can improvise the existing password based system. In this system, it makes use of secret data to identify the user instead of a login ID[4]. The system then asks the user to select a correct login ID from the available IDs. As the system does not accept a login ID during the authentication process, a stolen password cannot be used for gaining access to the system unless the attacker provides accurate information i.e., mind-metrics token. This step is to improve the security of the system over single or double password systems. The users can change their passwords before the attackers gain access to the system. This system does not need any special infrastructure and can be implemented easily, where biometrics systems does not work effectively. This Mind-metrics scheme separates the identification server and the verification server[16,17].

CONCLUSIONS

Survey has been done on existing authentication techniques like one factor authentication, two factor authentication, and three factor authentication systems. In order to reduce the failure rate of existing authentication factors, a new procedure for emergency authentication called fourth factor authentication is required. If in any case, any of the authentication factor fails, user can be proved authenticate by means of the fourth factor, thereby reducing the usage of multiple factors.

REFERENCES

1. Haga, W. J. and M. Zviran, Cognitive Passwords: From Theory to Practice, Data Processing and Communications Security. In *8th Conference on exploring the challenges on e-business*, 2009; 13(3): pp. 19-23.
2. Moshe Zviran, Zippy Erlich, Identification and authentication: technology and implementation issues. In *Communications of AIS,* Volume 17, Article 4.

[3] John Brainard, Ari Juels, Ronald L. Rivest, Michael Szydlo, Moti Yung, Fourth Factor Authentication: Somebody You Know. In *Proc. of the 13th ACM Conference on Computer and communications security,* 2006; pp. 168-178.

4. John Brainard, Ari Juels, Burt Kaliski, Michael Szydlo, A new two-server approach for authentication with short secrets. In *Proc. Int, conf. on USENIX Security Symposium* , 2003; pp 14.
5. Stuart Schechter, Serge Egelman, Robert W. Reeder, It's Not What You Know, But Who You Know: A social approach to last-resort authentication, CHI 2009, Boston, USA
6. Stephen S. Hamilton, Martin C. Carlisle, and John A. Hamilton, A Global Look at Authentication. In *Proc. of IEEE Workshop on Information Assurance and security workshop*, 2007.
7. Fadi Aloul, Syed Zahidi, Wassim El-Hajj,

Two Factor Authentication Using Mobile Phones, In *The 7th IEEE/ACS International Conference on Computer Systems and Applications*, AICCSA, 2009.

8. Muthucumaru Maheswaran, Bijan Soleymani, Social Authentication Protocol for Mobile Phones. In *Proc. IEEE 16th Int. Conf. on Computational Science and Engineering*, 2009; pp: 436-444.
9. Brostoff and A. M. Sasse, Ten strikes and you're out: Increasing the number of login attempts can improve password usability. In *Proc. Int. Conf on HCI and Security Systems*, 2003.
10. Magno, Marianna B. Monterey, Survey of user authentication mechanisms. Naval Postgraduate School: Monterey, CA 93943-5000.
11. Yang, G., Wong, D. S., Wang, H. & Deng, X, Two-factor mutual authentication based on smart cards and passwords. *In Journal of Computer and System Sciences,* 2008; pp. 1160-1172.
12. Payas GUPTA, Exploiting Human Factors in User Authentication, Institutional Knowledge at Singapore Management University, 2013.
13. Xinyi Huang, Yang Xiang, Ashley Chonka, Jianying Zhou, Robert H. Deng, A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems. In *IEEE Transactions on Parallel and Distributed Systems,* 2011*;* pp 1390-1397
14. Jiøí Sobotka, Radek Doležel, Multifactor authentication systems. In electro revue, vol. 1, 2010.
15. Fabian Monrose, Michael K. Reiter, Qi Li, and Susanne Wetzel, Cryptographic key generation from voice. In *Proc. Int. Conf on Security and Privacy*, 2001.
16. Gkarafli, S. & Economides, An experimental survey and comparison of proof by knowledge authentication techniques. *International Journal of Applied Research on Information Technology and Computing*, 2010.
17. Sung Choi and David Zage, Addressing Insider Threat using "Where You Are" as Fourth Factor Authentication, In *IEEE International Carnahan Conference on Security Technology,* 2012; pp. 147-153.
18. Xinyi Huang, Yang Xiang, Ashley Chonka, Jianying Zhou, Robert H. Deng, A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems. In *IEEE Transactions,* 2011*;* pp 1390-1397.