Trusted Device along with Trusted Location and Biometry based Authentication Method

Md. Tanvir Rahman
Lecturer, Department of CSE
Daffodil International University
Dhaka, Bangladesh

Taslima Ferdaus Shuva
Lecturer, Department of CSE
Daffodil International University
Dhaka, Bangladesh

K. M. Akkas Ali
Associate Professor, IIT
Jahangirnagar University
Dhaka, Bangladesh

ABSTRACT

Now a days wireless networks and smart devices are getting popularity day by day. With the growing availability of the internet, these facilities have made our life much easier by providing a lot of automated services. Hence to make the user experience much convenient, service providers allow accessing these services through a variety of devices in many ways. Although these technological inventions are blessings to us, client authentication is of the critical issues as intruders may acquire unauthorized access and use their advanced knowledge to impersonate the actual user and steal valuable information. Single factor authentication, e.g. password, being the first authentication approach is no longer considered as secure whereas two factor authentication provides a bit higher protection level by extending a factor. Apart from these, a new concept called multi factor authentication is the most secured approach that requires a combination of two or more different factors. In this paper, a multi factor authentication method is proposed that includes knowledge, possession, location and inherence which can add a new dimension in the security area of user authentication in a hassle free manner.

General Terms

Entity Authentication

Keywords

Multi-factor authentication, Biometric, Trusted Device, Trusted Location, GPS

1. INTRODUCTION

In recent years the Internet has become a part and parcel of our daily life. It is a worldwide interconnection of the mainframe, personal and wireless networks that use the internet protocol suite to establish their communication link. It can be also considered as a network of networks consisting trillions of public, private, governmental and non-governmental networks of local to global scope, linked by a broad array of networking technologies. Apart from this, organizations are also expanding their network on a larger scale than ever before and internet is being used for the default interconnectivity of these networks.

Presently the number of Internet users, doing online commerce, knowledge sharing, business transaction, social networks etc., is more than 2.4 billion. As a result, the need for security and enhanced privacy has become an important issue. Therefore, the three vital security issues that take place every now and then in internet communications are identification, authentication and authorization. These three interrelated concepts shape the core of a security system. Identification is the process that helps to recognize a claimed entity which may be a person, a machine or another asset such as a software. Authentication is the process through which a claimant proves that she is who she claims she is. Lastly after identification and authentication of a claimant, authorization takes place to determine the particular access to the system [1].

Among many types of verification approaches, most of the systems usually rely on static passwords for user authentication [2]. Apart from this, users have also a tendency to use simple and obvious passwords which will be easily guessable and even these same passwords are used for multiple accounts. Sometimes users keep these passwords written in a notebook or store these into a system and even they don’t change their password unless and until they are forced to do so [3, 4]. As a result, hackers, identity thieves and intruders can gain unauthorized access to the system by utilizing sophisticated tools and techniques or attacks like shoulder surfing attack, dictionary attack, guessing attack, snooping attack or even brute force attacks. Therefore, in order to augment the security sometimes very complex password policies are enforced to the user by requiring a minimum number of characters, a combination of lowercase and uppercase letters, an inclusion of digits or non-alphanumeric symbols and even in some cases frequent password expiration. This often results in an unacceptable conflict between security and user satisfaction as they suffer a lot of problems during password selection [5], their consonance [6, 7] and management [8, 9]. These problems lead the user to choose the easiest password [10].

In order to address the issues for single factor authentication, multi-factor authentication has emerged to enhance the security by utilizing more than one authentication factor, as opposed to only a password [11, 12]. Historically, ‘Two Factor Authentication (TF-A)’ has been used mostly in governmental as well as non-governmental and financial enterprises where information security has become a primary concern for users. Recently, most of the service providers such as Facebook, Google, Twitter, Dropbox, etc. being motivated by the increasing number of password hacking have also provided their users an option of using two-step verification which is a TF-A. But the TF-A is not a perfect solution as it is often vulnerable to man-in-the-middle attack, forgery or Trojan-based attacks and it is not fully effective to defend phishing [13]. Furthermore, TF-A suffers from user satisfaction as it requires users to carry out additional actions for authentication and verification such as entering a one-time password or verification codes.

In this paper, an efficient multi-factor entity authentication method is proposed which comprises four factors such as knowledge (something that user knows, e.g. password), possession (something that user owns, e.g. trusted device), location (somewhere the user is, e.g. trusted location) and inherence (something that qualifies the user, e.g. biometrics) in a way which will provide a hassle free authentication approach and yet secured.

2. CONCEPTS AND DEFINITION OF AUTHENTICATION

Authentication is a technique through which the verifier proves the identity of a claimant based on some type of witnesses. In this approach, the claimant whose identity is to be proved can be a person, a process, a client or a server and the party that tries to prove the identity of the claimant is called the verifier. The main differences between message authentication and entity authentication are that entity authentication is real time where message authentication is not and secondly entity authentication proves the identity of a claimant for the entire duration of a session where message authentication does not and this process has to be repeated for each new message [14].

2.1 Authentication Factors

There are some ways through which someone can be authenticated into a system. These ways are called as authentication factors. Each authentication factor covers a range of choices to authenticate the claimant prior to give the access or establish a chain of authority. Some of the widely recognized authentication factors for human are as follows:

2.1.1 Something the claimant knows

A secret that the claimant knows only, e.g. a passphrase, a security question, a password, a partial password, a pin, a pattern, a secret key, a private key etc.

2.1.2 Something the claimant owns

Something which can help proving the claimant's identity, e.g. an ID card, a smartphone, a smart card, a credit card, a USB token etc.

2.1.3 Something the claimant inherits

Inherent characteristics of the claimant, e.g. fingerprints, retinal pattern, voice, facial characteristics, hand geometry etc.

2.1.4 Something the claimant can do

An activity that proves the claimant, e.g. a signature, a gesture etc.

2.1.5 Somewhere the claimant is

Location of the claimant, e.g. a geographical point, a geographical zone.

Using more than one authentication factor is sometimes referred to as strong authentication but the strength of the system relies on the strength of the authentication methods underneath each factor [15].

2.2 Authentication Types

2.2.1 Single Factor Authentication

Single-factor authentication is a process to grant access of a claimant into the system through only one category from the various authentication factors, i.e. something the claimant knows. Simple password based authentication can be termed as the most common example of SF-A [16].

2.2.2 Two Factor Authentication

Two-factor authentication also called as two-step verification aims at enhancing the security by requiring the claimant to provide an additional authentication factor than the traditional password based authentication [17]. The two factors constituting the TFA is usually a combination of something that claimant knows and something the claimant owns.

2.2.3 Multi Factor Authentication

Multi-factor authentication is a special type of security framework where the claimant has to gain the authentication by successfully presenting several types of evidence. Typically, in an MF-A at least two of the authentication factors are used [18].

2.3 Basic Authentication Steps

Basic authentication requires that the authentication server requests predefined credentials from the claimant and verify those credentials with a database of authorized users in a specified or default realm.

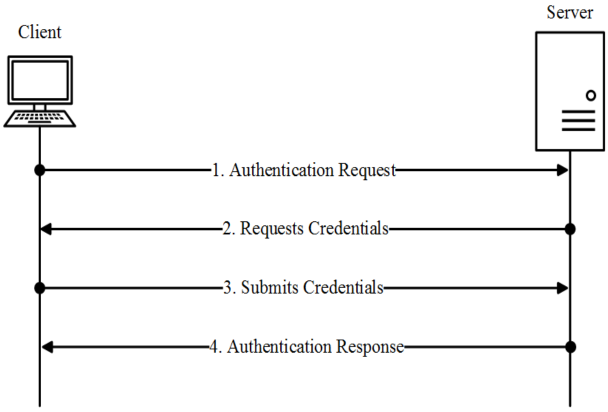

Fig 1: Basic authentication steps

Figure 1 describes the basic steps where the claimant provides the required credentials requested by the verifier in order to be authenticated.

3. EXISTING AUTHENTICATION METHODS

The most common authentication approach is the use of traditional username and password although it has a lack of security. The authors of [19] found that users demand a transparent authentication method that results in a strong security. In order to provide such strong authentication security, the password policy plays a vital role. A study of the impact on usability and password policies shows that complex password generally improves the security but decreases average password entropy and user satisfaction [20].

In 2004, the authors of [21] proposed an authentication scheme based on a generalized EIGamal signature scheme which provides mutual authentication and also enables users to change or update their passwords freely without the help of a remote system. But the main drawback of this approach is an invader can reveal the previous session keys by means of disclosed secret parameters. In order to address this issue, a forward secured user authentication scheme is proposed [22]. Later on, another mutual authentication scheme is proposed which is based on smart cards and passwords under trusted computing [23]. In this approach to authenticating identities, hash functions are used and for platform verification, remote attestation is used. Analysis showed that the proposed scheme in [23] can resist most of the possible attacks and fulfills several security goals such as a secure session key agreement, user identity anonymity, password free changing, platform certification updating. As the smart card still has the problem of traceability and desynchronization attack, a robust user authentication and key agreement scheme is proposed which is suitable for ubiquitous computing environments which achieved all goals of security [24].

The authors of [25] proposed a secure and stable protocol using multi-factor authentication. To provide extra security along with traditional username and password TIC (Transaction Identification Code) and SMS (Short Message Service) are included. On the other hand, instead of using TIC the authors have suggested using OTP (One Time Password) along with SMS to have more secure and efficient authentication [26].

Graphical passwords have also been proposed as an authentication method as it provides very convenient user experience rather than using complex passwords as well as time consuming OTP [27, 28]. A series of authentication methods using graphical passwords are proposed in [29].

The use of biometrics such as fingerprint, facial scan, hand geometry has been used in recent authentication frameworks as it provides convenient and easy to use secure person authentication method [30, 31]. Another implicit authentication method is Arm Swing that is the way in which user generally swing their hands while doing other works. It is also called as Gait Authentication. It is basically developed for mobile phones which is based on movements of a person like walking, moving hands [32].

The authors of [33] have proposed a dynamic authentication approach called Zero-Effort Bilateral Recurring Authentication (ZEBRA) which is a token-based authentication scheme that authenticates users based on their interactions (e.g. typing or scrolling) with the device. In this approach, the user needs to wear a bracelet that has a built-in accelerometer, gyroscope and radio. When the user interacts, the bracelet records the movement and after processing it sends data to the system.

4. PROPOSED METHOD

The proposed authentication framework uses four authentication factors where the verifier tries to find from where the request is coming then from which device, and later on who is doing that request followed by the initial authentication of the claimant.

First of all, the claimant has to provide his/her initial credentials (i.e. username and password) in order to proceed. If the credentials are matched, then the verifier checks whether the location from where the request is coming is trusted or not. If it is ok, then the verifier checks whether the MAC address of that requesting device matches any one of the trusted devices in the list. If so, then the system will require a biometric password of the claimant to authenticate. If it matches, then he/she is granted to access otherwise rejected.

For the location verification, the user can use trusted point or trusted zone depending on the condition and for the biometric verification user can use fingerprint, face or voice as these features are available in recent smart devices.

Figure 2 describes the flow diagram of the proposed authentication framework.

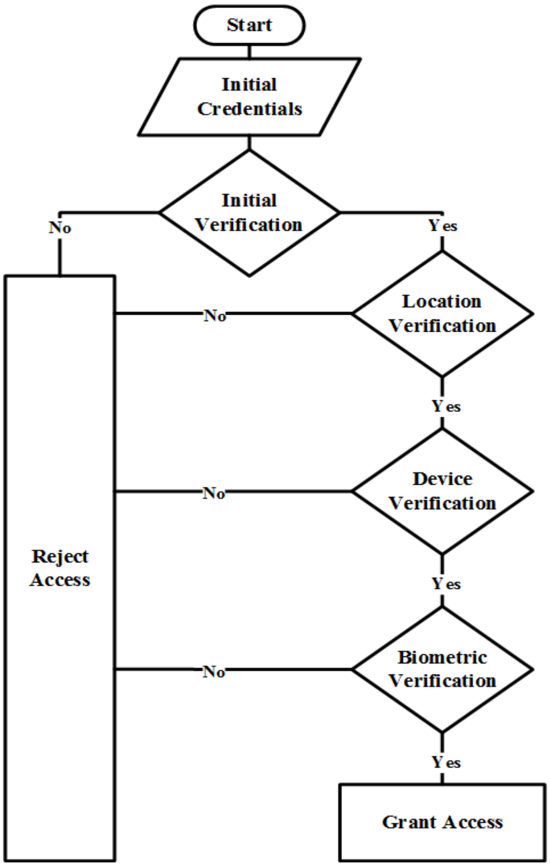

Fig 2: Flow diagram of proposed framework

5. CONCLUSION

Single factor authentication has become obsolete due to the extensive amount of account hacking and so it is not considered safe anymore. Multi-factor authentication method has recently been introduced to meet the strong security demand of online communications and services. Although the multi-factor authentication method performs well, it requires a set of additional tasks to be completed that involves the user. These additional tasks sometimes create hassles as users always seek for the easiest approach.

The proposed authentication approach can satisfy both users and service providers as it is simple and the only thing a user has to remember is a password. As a result, it is more likely the traditional single factor authentication method but yet it uses four factors which results in a convenient way to authenticate a user.

The research work can further be extended to evaluate the performance with other multi-factor authentication methods in real life scenarios.

6. REFERENCES

[1] P. Kotzanikolaou and C. Douligeris, “Network Security Current Status and Future Directions”, John Wiley & Sons, ch.1, 2007.

[2] D. Florencio, C. Herley “A Large-Scale Study of Web Password Habits”, in Proceedings of the 16th International conference on the World Wide Web, pp 657-666, 2007.

[3] E. F. Gehringer “Choosing passwords: Security and Human factors” in IEEE international symposium on

Technology and Society, (ISTAS'02), pp. 369 - 373, 2002.

[4] J. Yan, A. Blackwell, R. Anderson, A. Grant "Password Memorability and Security: Empirical Results" in IEEE security and privacy, vol. 2, no. 5, pp. 25 - 31, 2004.

[5] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley, "Does my password go up to eleven?: the impact of password meters on password selection", in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2379-2388, 2013.

[6] A. Karole, N. Saxena, and N. Christin, "A comparative usability evaluation of traditional password managers", in Proceedings of the 13th international conference on Information security and cryptology, pp. 233-251, 2011.

[7] R. Weiss and A. D. Luca, "Passshapes: utilizing stroke based authentication to increase password memorability", in Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges, pp. 383-392, 2008.

[8] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people: measuring the effect of password composition policies", in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2595-2604, 2011.

[9] E. von Zezschwitz, A. De Luca, and H. Hussmann, "Survival of the Shortest: A Retrospective Analysis of Influencing Factors on Password Composition", in Human-Computer Interaction – INTERACT 2013, vol. 8119, pp. 460-467, 2013.

[10] A. Adams and M. A. Sasse, "Users are not the enemy", in Communications of the ACM, vol. 42, no. 12, pp. 40-46, 1999.

[11] J. Reno, "Multifactor Authentication: Its Time Has Come", in Technology Innovation Management Review, vol. 3, no. 8, pp. 51-58, 2013.

[12] O. S. Adeoye, "Evaluating the Performance of two-factor authentication solution in the Banking Sector", in International Journal of Computer Science Issues, vol. 9, no. 4 , 2012.

[13] B. Schneier, "Two-factor authentication: too little, too late", in Communications of the ACM – Transforming China, vol. 48, no. 4, pp. 136, 2005.

[14] B. A. Forouzan, "Data Communication and Networking (4th edition)", Tata McGraw-Hill Education, pp. 976, 2006.

[15] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, J. J. Schwartzmann, "A Review on Authentication Methods", Australian Journal of Basic and Applied Sciences, vol. 7, no. 5, pp. 95-107, 2013.

[16] S. Peisert, E. Talbot, T. Kroeger, "Principles of authentication", in Proceedings of the workshop on New security paradigms workshop (NSPW '13), pp. 47-56, 2013.

[17] E. D. Cristofaro, H. Du, J. Freudiger, and G. Norcie, "Two-Factoror not Two-Factor? A Comparative Usability Study of Two-Factor Authentication", in NDSS Workshop on Usable Security(USEC), 2014.

[18] K. Abhishek, S. Roshan, P. Kumar, R. Ranjan, "A Comprehensive Study on Multifactor Authentication Schemes", in Proceedings of the Second International Conference on Advances in Computing and Information Technology (ACITY), vol. 2, pp. 561-568, 2013.

[19] S. Furnell, N. Clarke, and S. Karatzouni, "Beyond the pin:
Enhancing authentication for mobile devices", in Computer Fraud and Security, vol. 2008, no. 8, pp. 12-17, 2008.

[20] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people: measuring the effect of password composition policies", in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2395-2604, 2011.

[21] E-J. Yoon, E.-K. Ryu and K-Y. Yoo, "Efficient remote user authentication scheme based on generalized ElGamal signature scheme," in IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 568-570, 2004.

[22] B. Wang and Z-Q. Li, "A Forward-Secure User Authentication Scheme with Smart Cards", in Internation Journal of Network Security, vol. 3, no. 2, pp. 116-119, 2006.

[23] L. Yang, J-F. Ma, Q. Jiang, "Mutual Authentication Schemes with Smart Cards and Password under Trusted Computing", in International Journal of Network Security, vol.14, no.3, pp. 156–163, 2012.

[24] R-C. Wang, W-S. Juang, and C-L. Lei, "Robust authentication and key agreement scheme preserving the privacy of secret key", in Computer Communications, vol. 34, no. 3, pp. 274-280, 2011.

[25] A. Tiwari, S. Sanyal, A. Abraham, S. J. Knapskog, S. Sanyal, "A Multi-Factor Security Protocol for Wireless Payment – Secure Web Authentication Using Mobile Devices", in Proceedings of the IADIS International Conference on Applied Computing, pp. 160-167, 2007.

[26] A. Al-Qayedi, W. Adi, A. Zahro and A. Mabrouk, "Combined Web/mobile authentication for secure Web access control," in Wireless Communications and Networking Conference, vol. 2, pp. 677-681, 2004.

[27] S. Vaithyasubramanian, A. Christy, "A practice to create user friendly secured password using CFG", in International Conference on Mathematics and Engineering Sciences, Chitkara University, Punjab, pp. 39, 2014.

[28] S. Vaithyasubramanian, A. Christy, "Generation of Array Passwords Using Petri Net for Effective Network and Information Secutity", Advances in Intelligent Systems and Computing, vol. 1, pp. 189-200, 2014.

[29] A. P. Sabzevar and A. Stavrou, "Universal Multi-Factor Authentication Using Graphical Passwords," in International Conference on Signal Image Technology and Internet Based Systems, pp. 625-632, 2008.

[30] Y. Sui, X. Zou and E. Y. Du, "Biometrics-Based Authentication: A New Approach," in Proceedings of 20th International Conference on Computer Communications and Networks, pp. 1-6, 2011.

[31] S. S. Mudholkar, P. M. Shende, M. V. Sarode, “Biometrics Authentication Technique for Intrusion Detection Systems Using Fingerprint Recognition”, in International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), vol. 2, no. 1, 2012.

[32] L. Yuexiang, W. Xiaobo and Q. Feng, “Gait Authentication Based on Accelerating Singnals of Ankle: in Chinese Journal of Electronics, vol. 20, no. 3, 2011.

[33] S. Mare, A. M. Markham, C. Cornelius, R. Peterson and D. Kotz, “ZEBRA: Zero-Effort Bilateral Recurring Authentication”, in IEEE Symposium on Security and Privacy, pp. 705-720, 2014