International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

A Comparative Analysis of Various Multifactor Authentication Mechanisms

B. Kharthik Kumar Reddy[1] , Dr. B. Indira Reddy[2]
*[1]M-Tech, IT, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India
[2]Professor, IT, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India

ABSTRACT

Due to advancements and improvements in internet and communication systems, more people are relying on internet to store their confidential information. Earlier the idea of static passwords was being used but most of the passwords are weak and easily guessable. According to a survey ninety percentage of passwords that are used by people are poor very poor or keywords of their personal information, which makes easy for attackers and intruders to guess passwords in different combinations using brute-force attack. Thus the idea of multi-factor authentication introduced in the world instead of this remote client authentication mechanism. It hardens the security of network and make difficult for the attackers to crack the system. In these mechanisms, user needs to provide extra information along with username and passwords. Most popular is one-time passwords that are generated randomly and valid only short period (30 to 60 seconds). In this paper, review of various multi-factor authentication schemes has been performed to compare various authentication mechanisms.

Keywords: Multi-factor authentication, One time passwords, Static passwords, Short message service, Time base done time passwords (TOTP) and Image based and Finger print authentication.

I. INTRODUCTION

The internet and mobile communications have been developing and related application or services for managing money and personal information are increasing in number day by day. Thus, now-a-days people rely more on internet to store the confidential and important data. However, there is a risk that private data may be wiretapped. Therefore, it is necessary to authenticate users and in order to keep this web data safe on cloud almost every client and server implement cryptographic techniques to encrypt this sensitive data, as well as verify entities at the other end of the connection. Thus if more confidential data is to be stored online, it is necessary that the network security should stay up to date with modern attacks. However, online users continue to use weak and easily guessable passwords like birth dates, partner names, children names etc. and they are typically only letters. Also, if the user sends the same password every session, an attacker can easily masquerade as a user, because the attacker may succeed in getting the user's password through internet. So, it is becoming clear that passwords are not sufficient means to protect the online accounts. Various authentication schemes are being in use today to harden the security of online data or information. Authentication also plays an important role when the transactions are related to money i.e. in financial transactions. One of the common

CSEIT1835225 | Received : 15 June 2018 | Accepted : 26 June 2018 | May-June-2018 [(3)5 : 1098-1103]

authentication scheme used in financial services or transactions is using a hardware token.

They are vulnerable to some frauds like swindlers (attackers) make use of skimmers that are devices used to capture data from the magnetic stripe of the card issued by the bank or any financial institution. Multi layering of multi factor authentication is also important in hardening the security of financial services.

USERNAMES AND PASSWORDS:

The traditional and oldest method for providing authentication is using usernames and passwords. Most of the websites use this method to provide security to their client's personal data. The username is used to identify which online account does user or client wants to access and passwords are used to prove the identity of that legitimate user. Passwords are stored on server side in encrypted form or using hash functions, also the username and passwords transmit in encrypted form over the secure connection. Thus if any intruder get access over the network, there is no worry about leakage of important information as it will not reveal any information about actual password. Even though it looks secure but in practical it is not as secure as an attacker can get original password of a client using brute force attack after a few combinations. Also, the user continues to use easy and guessable passwords, so it is recommended to use complex passwords or changing it repeatedly after short period of times.

These single static passwords are also very vulnerable to social engineering i.e. people may ask for passwords or can also guess them correctly. Some surveys carried out on various places have revealed that how easy it is to get people reveal their passwords very easily. Any attacker can also use these passwords to access their personal accounts otherwise one need to change their passwords repeatedly. A few emphasis have been given on usage of complex passwords like it's length should be minimum 8 characters, should have at least one numeric and one special symbol etc. But due to various vulnerabilities and attacks like phishing, man in the middle attack, brute force etc on static passwords, a need of hardening the security of online data and information stored by the users has been raised. Thus, after a few researches in the field of online security, a method has been proposed. In which the authentication of legitimate users have to be performed not only in a single step through a password but is to be performed in various steps by asking for more information about the user by the server. This gives rise to the introduction of Multi-step or Multi-factor authentication scheme.

MULTI FACTOR AUTHENTICATION:

Multi-factor Authentication is a method of computer access control which a user can pass successfully presenting various authentication stages. In this, instead of asking just single piece of information like passwords, users are asked to give some additional information which makes it more difficult for any intruder to fake the identity of the actual user. This additional information can include various factors like finger prints, biometric authentication, security tokens etc. It has emerged an alternative way to improve the security by requiring the user to provide with more than one authentication factor rather than only a single password. Authentication factors are of these kinds:

1. Knowledge – something that the user knows, e.g., a username and a password;

2. Possession – something the user has, e.g., a hardware token (as a security token);

Multi factor authentication can be performed in various ways, most common of them is using login credential with some additional information but a different technique also include authentication in which usage pattern of input data is used in determining the authenticity of user like the time taken by user to input his details, or the pressure exerted by the user's finger on the touch screen of the Smartphone may be calculated to find whether the login is done by the authenticate user or by any other attacker.

Mostly all the websites and online services are now-a-days implementing multi-step authentication to provide security to their customers. More recently, an increasing number of service providers like Google, Face book, Drop box, Twitter, LinkedIn etc. have also begun to provide their users with the option of enabling multi-factor authentication; this is motivated by the increase in number of hacking passwords. Multi layering of authentication is also becoming popular these days in which authentication is provided at various levels. Different kind of authentication technique is provided at each level like knowledge based biometric authentication etc. individually at each level. As a general, in multi-step users are required to provide some required information along with the login credentials'.

The organization of this document is as follows. In Section 2 (**Related Work)**, which gives the brief information about the various techniques that are used for the multi factor authentication .In Section 3 (**Conclusion**), the conclusion of the reviewed work is explained here and Section 4 shows the References that are referred for this work.

II. RELATED WORK

3. Inherence – something verifies the user is, e.g., fingerprints.

Uymatiao, Mariano Luis T., and William Emmanuel S. Yu (2014) have worked on Time-based OTP through secure tunnel (TOAST). They have collectively developed a mobile TOTP scheme using TLS seed exchange and encrypted offline keystroke[1]. The main objective of this research is to build upon existing cryptographic standards and web protocols to design an alternative multi-factor authentication cryptosystem for the web. It involves seed exchange to a software-based token through a login-protected Transport Layer Security (TLS/SSL) tunnel, encrypted local storage through a password-protected keystroke (BC UBER) with a strong key derivation function, and offline generation of one-time passwords through the TOTP algorithm. Authentication occurs through the use of a shared secret (the seed) to verify the correctness of the one-time password used to authenticate[7].

Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin and Jean-Pierre Seifert (2014) have worked on SMS based One Time Passwords that were introduced to counter phishing and other attacks against various internet services like in Banking Services[2]. Now days, these OTPs are used for authentication and authorization in various other applications. But they are also prone to very heavy attacks especially to Smartphone Trojans. Thus, they collectively study the security architecture of SMS OTP systems and study attacks. Also, they proposed a mechanism to secure SMS OTPs against common attacks and specifically against Smartphone Trojans[8].

Short Message Service based One Time Passwords In previous system, the security of online data was based on system authorization and authentication processes. The most simplest way of authenticating user is through usernames and passwords. Though the various well-known security issues, passwords are most-popular method for end-user authentication. The major advantage of SMS based OTP system is that it is compatible with any SMS-enabled mobile phone. Since the only thing a SMS-based system needs to provide to the server is the user's phone number.

Also, very few steps are involved in this technique and is the simplest way of generating one time passwords and even simpler in transmission of the unique codes. It also keeps the cost very low as a large customer already owns a mobile phone for purposes other than generating One Time Passwords. Because of these advantages most of the banking transactions like internet banking, Master/Visa credit or debit card transactions, enables an extra layer of security by providing an extra One Time Passwords (OTP) SMS verification. The problem with SMS-based OTP is that it is only as good as the mobile network of the user. If the network is slow, the user may be delayed from logging into account or even the received unique code may be expired. Thus, a user would either be delayed to get access to the service or may request to send a new one time password. Also, several attacks against GSM and 3G networks have shown that confidentiality for SMS messages cannot necessarily be provided[3].The one time passwords sent via SMS are always transmitted in plaintext which is more vulnerable to man-in-the middle attack. As SMS-OTP relies on single mode of communication between the users and the related web services and thus it is an in-band authentication.

Michiel Appelman, Yannick Scheelen (2012) have analysed on Google's 2-step verification login system. In which, Google asked for a verification code in combination with username and password. This unique verification code can be generated via three methods i.e. verification code can be sent via email or to the mobile phone through voice call or a text message. Another way is Google introduces a special Smartphone application that generates verification codes on users Smartphone that are valid only for 30 seconds of time[3].

Google introduces 2-step verification or authentication scheme in September 2010 for Google Applications users. After enabling this service user have to provide an extra verification code after logging into their Google accounts. This verification code could be received by a Short Message Service (SMS) text message or voice over text message, or even through a token or code generating application developed by Google. Google's 2-step verification requires something you have (like smart phone with Google authenticator installed to generate verification code) and something you know (that is the password of your Google account) that is required to access into your account. The verification code could be retrieved via a token generator on a Smartphone. These token based verification codes are generated using a time-based algorithm.

Subashini K., and G. Sumithra (2014) have worked on Secure multimodal mobile authentication using one time password. There are several issues when it comes to security concerns in these numerous and varying industries with one common weak link being passwords[4].

Michiel Appelman, Yannick Scheelen (2012) have analysed on Google's 2-step verification login system. In which, Google asked for a verification code in combination with username and password. This unique verification code can be generated via three methods i.e. verification code can be sent via email or to the mobile phone through voice call or a text message. Another way is Google introduces a special Smartphone application that generates verification codes on users Smartphone that are valid only for 30 seconds of time[3].

Google introduces 2-step verification or authentication scheme in September 2010 for Google Applications users. After enabling this service user have to provide an extra verification code after logging into their Google accounts. This verification code could be received by a Short Message Service (SMS) text message or voice over text message, or even through a token or code generating application developed by Google. Google's 2-step verification requires something you have (like smart phone with Google authenticator installed to generate verification code) and something you know (that is the password of your Google account) that is required to access into your account. The verification code could be retrieved via a token generator on a Smartphone. These token based verification codes are generated using a time-based algorithm.

Nitin Mujal, R. Moona (2009) described a secure and cost effective transaction model for financial services. As with the advent of the e-commerce, it has become much easier for the intruders or attackers to sit in non-descriptive location and quietly siphon away the money from the service users. Thus also the financial service outlets like Automated Teller Machine (ATM), Point of sale (PoS) terminal have also been an easy target. As the users are forced to trust a service outlet to be authentic but actually they can be spoofed and also a spoofed outlet can collect the account information of the users and can use the same to do financial transactions[5]. These outlets are also very expensive to implement. Thus a secure and cost effective model has been proposed to overcome various securities and cost related issues of financial service models. It is cost effective such that financial services can also reach to the rural population and contribute to rural development. It relies on public key infrastructure (PKI) architecture to provide ensures about both cost and security issues[6].

M.M. Mohammed, M. Elsadig (2013) provided a multi-layer of multi factors authentication model for Online Banking Services. The security risks of internet banking have always been a matter of concern for the service providers as well as for the users[9]. Various online environments like internet banking, electronic transactions and financial services have been analyzed to identify the characteristics and issues of existing authentication methods in order to present a user authentication level system model that is suitable for different online services. Multi-factor Authentication has been integrated with multi layer authentication techniques in order to produce a standard layered multi factor authentication model suitable for different online banking services suitable based on risk assessment criteria. The proposed model includes 5 levels such that each level contains one or combination of various authentication factors such as knowledge-based, possession based, or biometric based factors. The standard model is compared to multi layering guidelines and it shows improvement and fulfilment of authentication[10].

The RSA Secure ID authentication System consists of a token that can be hardware (e.g.- a USB dongle) or a software (a soft token) which is given to the computer user and it is used to generate one time unique passwords that lasts for a maximum of 60 seconds time span[12]. Generation of this one time password is done using encoded-random key that is known as seed. This seed is unique for each token and is loaded into their corresponding to RSA Secure ID server. Tokens are also available On-Demand, in which token codes or unique passwords can be sent to the user via email or text SMS, which eliminates the need of a provision of token to the user. In this authentication scheme, seed is the secret key used to generate unique passwords. It also allows token to be used as Smart Card-like device to store certificates securely. Hard Tokens are on the other hand can be physically stolen (like they can be stolen by social engineering attacks) from the authenticated end users. Also the user will not report immediately after the theft of the security token. The user will at least wait for one day before reporting the device as missing. This will give intruder a plenty of time to breach the protected system. However this could only occur if the unique username and password of account is known [14].

Generation of secure One Time Password based on Image Authentication The Image-based Authentication (IBA) is based on Recognition Technique. It is almost similar to text one time passwords as in this also the user is provided a shared secret as an evidence of his/her identity. However, text-based OTPs use alphanumeric characters to represent the secret and IBA uses visual information. When the user registers for the first time on the website, they are required to select a set of images that are easy to remember such as natural scenery, automobiles etc[11]. Every time a user login into the website or service, they are provided a grid of images randomly generated. Then, the user can identify the images previously selected by them. The user is authenticated by correctly identifying the password images. The category of images is stored by the authentication system on Image Identification Set (IIS). When a user login, the IIS for that user is only retrieved and is being used to authenticate that particular user. The human is more adept in retrieving or recalling a previously seen image rather than a previously seen text. In a study conducted at University of California at Berkeley, Image-based authentication (IBA) systems have been found as more user-friendly than usually used text-password systems[13].

Phillip H-Griffin(2015) describes a method for achieving strong, multi-factor and mutual authentication from a biometrics-based protocol for authenticated key exchange (B-AKE)[6].

Operation of the protocol relies on knowledge shared by communicating parties, extracted from data collected by biometric sensors. A Diffie-Hellman key-agreement scheme creates a symmetric encryption key using a weak secret, the extracted something-you-know data. This key protects the confidentiality of user credentials and other message data transferred during operation of the B-AKE protocol. If the message recipient possesses the same something-you-know information as the sender, a key is created, the message decrypted, and mutual authentication achieved. Biometric match data recovered from the encrypted message provides a second something-you-are authentication factor. The B-AKE protocol ensures users never reveal their knowledge or biometric credentials to imposter recipients or man-in-the-middle observers. DiffieHellman key establishment provides forward secrecy, a highly desirable protocol property, when participants choose fresh random values each time they operate the protocol[15].

III. CONCLUSION

In this article by reviewing the pros and cons of various available login authentication schemes, firstly we reported on already available multi-step authentication mechanisms, how they work, how they are used, where and why. A few popular multistep authentication schemes include: one time pass code or passwords received via SMS, one time codes generated by security token i.e. RSA Secure ID, Smartphone applications for generating verification code like Google authenticator and TOAST, using images as verification passwords i.e. Image based authentication. Almost every kind of authentication system discussed above is widely used today to provide security to the users. One Time Passwords are an efficient technique to generate passwords randomly each time for user. OTP prevent users from replay or eavesdropping attacks. These passwords are valid only for given timeframe thus there is no threat that they can be reused by an intruder to login to user account as they are invalid after one time use. One Time Passwords can be generated either online or offline but offline generation is better as it can also be generated even if there is no network connectivity and it also prevents from the man in the middle attack. Thus it will be better for the services or websites to use offline method of generating one time unique codes like Google Authenticator or TOAST as they provide more confidentiality and authentication tothe user on internet.

IV. REFERENCES

1. Uymatiao, Mariano Luis T., and William Emmanuel S. Yu. "Time-based OTP Authentication via Secure Tunnel(TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystroke." 4thIEEE International Conference on Information Science and Technology(ICIST), 2014,Pp. 225-229,IEEE,2014.
2. Muliner, C., Borgaonkar, R., Stewin, P.,Seifert, J., "SMS-based One-Time Passwords: Attacks and Defense", volume 7967,Pp. 150-159 Springer-Verlag Berlin Heidelberg 2013.
3. Appelman, M., Scheelen, Y., "Analysis of Google's 2step Authentication",University of Amsterdam, May 2012, www.scribd.com/doc/95267199/Analysis-ofGoogle-s-2-StepVerification#scribd
4. Subashini, K., and Sumithra, G., "Secure multimodal mobile authentication using one time password." 2nd International Conference on Current Trends in Engineering and Technology (ICCTET), 2014, pp. 151155. IEEE, 2014.
5. Munjal N., Moona R., "Secure and Cost effective Transaction Model for Financial Services", International Conference on Ultra Modern Telecommunications and Workshops, 2009, Pp. 1-6, IEEE, ICUMT'09.
6. Phillip H. Griffin[2015] Biometric Knowledge Extraction for Multi-Factor Authentication and Key Exchange.
7. Studying on Internet of Things based on Fingerprint Identification,Huang hongbo, Wang Huan[2010] Zhongkai University of agriculture and engineering Guangzhou.
8. Steven M.Bellovin [2013]Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks.
9. Robust Multi-Factor Authentication for Fragile Communications Xinyi Huang, Yang Xiang Senior Member, IEEE, Elisa Bertino, Jianying Zhou, and Li Xu Member, IEEE[2013]
10. Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things Burak Kantarci, Senior Member, IEEE, and Hussein T. Mouftah, Fellow, IEEE[2014].
11. Towards secure cloud-centric Internet of Biometric Things Burak Kantarci, Senior Member, IEEE, Melike Erol-Kantarci Senior Member, IEEE, Stephanie Schuckers Senior Member, IEEE[2015]
12. Authentication and Access Control in the Internet of Things Jing Liu and Yang Xiao, C. L. Philip
13. Multi Factor Authentication Using Mobile Phones by Fadi Aloul1, Syed Zahidi1, Wasim El-Hajj2[2009]
14. A MULTI-FACTOR SECURITY PROTOCOL FOR WIRELESS PAYMENT- SECURE WEB AUTHENTICATION USING MOBILE DEVICES

Ayu Tiwari, Sudip Sanyal ,Ajith Abraham, Sugata Sanyal[2014].

15. Biometric-Rich Gestures: A Novel Approach to Authentication on Multi-touch Devices,NapaSaeBae,KowsarAhmed,KatherineIs bisterandNasirMemon[2012].
16. Identity-Based Authentication Scheme for the Internet of Things Ola Salman Sarah Abdallah Imad H. Elhajj Ali Chehab Ayman Kayssi[2016].
17. Remote Password Authentication Scheme with Smart Cards and Biometrics byChun-I Fan*, Yi-Hui Lin, and Ruei-Hau Hsu [2015]
18. Robust Multi-Factor Authentication for Fragile Communications Xinyi Huang, Yang Xiang Senior Member, IEEE, Elisa Bertino, Jianying Zhou, and Li Xu Member, IEEE[2012].