International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Web Application based Authentication Schemes to Resist Password Reuse and Password Stealing Attacks

Tanzila Maqsood Mirza[1], Shrikant R. Tandle[2]

[1]SRTM University, Department of CSE, M. S. Bidve Engineering College, Latur, Maharashtra, India

[2] Professor, SRTM University, Head of Department of CSE, M. S. Bidve Engineering College, Latur, Maharashtra, India

Abstract: ***Passwords are the most crucial elements to all digital secrets. Passwords remain the most largely used authentication method despite their renowned security flaws. Password is a secret term or a phrase that a person must know before being given consent to enter a place. The topmost source for user authentication was certainly Text passwords which people select while registering accounts on a website. The easier the password is for the owner to recollect usually means it would be easier for an invader to predict. And also the security of system can be reduced by passwords that are problematic to recall. Security is the major concern with usability. Security strategies need to be technologically advanced to protect information from unauthorized access. Passwords as well as the secret programs are used between users and information systems for protected user. Playing an energetic role in security, passwords that are easily guessed are links to vulnerability. They permit the intruder to put system assets knowingly nearer to access them, other versions on neighboring machineries and probably even administrative privileges with changed threats in addition to susceptibilities (e.g., phishing, key logging and malwares). In order to reduce the damage caused by phishing and other attacks, governments, banks and other industries are using One-Time Password schemes. This project provides a user authentication protocol named oPass which leverages a user's cell phone and short message service to thwart password stealing and password reuse attacks [13]. Through oPass, users only need to remember a long-term password for login on all websites [13].oPass only requires each participating website possesses a unique phone number[13], and involves a telecommunication service specialist in registration and recovery phases. But existing system entirely depends on telecommunication service provision and users contact number. User will obtain the One Time Password (OTP) with the help of prompt messaging service existing in internet .User can access their personal accounts using this OTP. The purpose of this system is to introduce the concept and methodology which helps users and organizations to implement stronger password procedures. oPass is efficient and affordable compared with the conformist web authentication mechanisms. The spasms over the complete systems are controlled through the addition of Secured Shared Key Sharing Mechanism as a contribution .TSP delivers the shared key to both server and user. The shared key can be hacked by the invader which affects the security of the authentication system. More security can be provided by sending the shared key secretly. User and server will generate the public and private key pair using the asymmetric key generation algorithm. Encryption of the Shared key is done by the TSP using the public key of the user when send to the user. Decryption is done by the user with the private key available with it. Hence the attack over the entire system is controlled through the addition of Secured Shared Key Sharing Mechanism. It gives rise to the safety level of the system. Proposed methodology is fewer susceptible to offline spasms, and this will provide robust shield against password stealing. Our system is less cost effective and better security apparatus against attacks.***

Keywords: Passwords, User authentication, Security, One time password, Secured shared key sharing mechanism.

1. Introduction

Today we are keeping all information digitally. Just consider the case of monitory transactions, know-how banks or anything; passwords are the key to all digital secrets. Password based user authentication can defend against dictionary attacks and brute force attacks if users opt for strong passwords to provide enough entropy. The complex methods that attackers can use to gain access to your personal information are becoming more easily accessible to wrong doers and are increasingly effective. It is essential to escape the common mistakes that give these individuals the opportunity to exploit your personal data. One of the common mistakes is that most users choose using a weak password. Selecting a weak password is similar to closing your front door but not locking it. A password is weak if it can be guessed easily. Another decisive problem is that users are using the same password for every account. This is a security concern because if an invader predicts or crashes a password for single account, he or she can access all your accounts. Even if the attacker acquires the password for a nonsensitive account; he or she can reuse it on sites where, for example billing, payment, shipping address and other private information is stored. Password reuse is the reason for users to drop the sensitive information stuffed into several websites if a hacker gains one of their passwords. This type of attack is known as the password reuse attack. Using the same pattern for your passwords is also risky. By learning your existing password structure, invaders can upsurge their chances of predicting passwords for critical websites such as your bank account or your company's email account. All the above issues are as a result of the bad part influence of human factors. Therefore, it is essential to take human factors into note when designing an individual authentication protocol. Usually, password-based user authentication can resist brute force [13] and dictionary attacks if users select strong passwords to provide sufficient entropy [13]. Regrettably, the password entropy that users can easily memorize seems inadequate to store unique and protected passwords for all these accounts causes users be likely to reuse passwords across different websites. Florencio and Herley specified that a user reuses a password

Licensed Under Creative Commons Attribution CC BY

across 3.9 various websites regularly [13]. Hence, passwords are a primary target of attackers for economically-inspired deeds with those pointing online bank accounts and identity theft. In order to save our information, we have to preserve our passwords first. If our passwords are not secure, an invader can take advantage to enter a particular account and can gain a criminal entrance. However, all passwords are important because wrongdoers can gain the confidential information you stored online and use it for their benefit. Customers enjoy the benefit of storing their billing and shipping addresses information along with their credit card information. An attacker can perform the attack in many ways. He can pretense himself as a legitimate user by misrepresenting the information, can mount key loggers or malwares, can perform spoofing or phishing attacks etc. There are lots of zones where the network security issues originate.

Upto now, researchers have studied a variety of skills to trim down the destructive impact of human factors in the authentication procedure. Since humans can easily remember graphical passwords than text passwords, many graphical password strategies were designed to deal with human's password recall problem [13]. Hence, Password management tools were designed. Strong passwords were automatically generated by these tools, which sermons password reuse and password recall attacks. Here, users have to memorize a master password to access the password management tool. Another attractive strategy is three-factor authentication. It is a method of computer access control in which user is granted access after successfully presenting several pieces of evidence to an authentication mechanism; of following categories: information (something user know); ownership (something user have), and inherence (something users are).To pass the authentication, the user must input a password and provide a pass code generated by the token (e.g., RSA SecureID) [13], and scan her biometric features (e.g., fingerprint or pupil) [13]. Another most eye-catching and appropriate approach is two factor authentications. It is an authentication procedure in which user has to provide two means of identification from diverse categories; one is a personal token, such as a card, and second is the memorized security code. Users basically forget to carry the token is the disadvantage.

OTP or one time passwords are very popular on transaction websites. This method has specifically become very much beneficial in validating users and authentication in real time. A one-time password (OTP) is an auto generated numeric or alphanumeric sequence of letterings that validates the user for a solo transaction or period. An OTP is safer than static passwords, especially a user-created password, which is typically weak. OTPs may substitute verification login information or may be used adding to it, to add an additional security layer. One time passwords assist as a very decent user authentication method .One-Time Passwords are valid for a fixed time period and is of no use once the user logs in, making them exceptionally useful against spyware such as key logging programs. Strong authentication systems discourses the boundaries of static passwords by integrating an added layer of security, a one-time password (OTP) strategy, to guard system entrance and end users digital characteristics. This will add an security level and it will be tremendously puzzling for an invader to access unlicensed data, grids or online accounts.

2. Literature Survey

Thus far, researchers have investigated a variety of technologies to trim down the negative influence of human factors in the authentication procedure. In [1], M.Wu, S. Garfinkel, and R. Miller, proposed an authentication protocol which uses a mobile phone as a hand-held authentication token, and a security proxy which allows the system to be used with unmodified third-party web services. Here the system is both secure and highly usable. The security of the system depends on SMS, which are encrypted with A5/1. However, algorithm A5/1 has been broken, and the system is also vulnerable to cellphone theft. .In [3], J. A. Halderman, B. Waters, and E. W. Felten have proposed a technique that uses strengthened cryptographic hash function to compute secure passwords for arbitrarily many accounts while requiring the user to memorize only a single short password. This mechanism functions entirely on the client; no server-side changes are needed.

In [4], B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell have describe a browser extension, PwdHash that strengthens web password authentication and transparently produces a different password for each site, improving web password security and defending against password phishing and other attacks. Since the browser extension applies a cryptographic hash function to a combination of the plaintext password entered by the user, data associated with the web site, and (optionally) a private salt stored on the client machine. In [5], K.-P. Yee and K. Sitaker have described a tool named Passpet which improves both the convenience and security of website logins through a combination of techniques. Passpet uses password hashing that helps users to manage multiple accounts by turning a single memorized password into a different password for each account

In [7], B. Parno, C. Kuo, and A. Perrig, have proposed a mutual authentication system named Phoolproof, prevention against phishing attack. Here, mobile devices are used as an authentication tokens to build an anti-phishing mechanism, called Phoolproof, via mutual authentication between users and websites. To log on the website, a user should provide the issued public key and username/password combination. Again, Phoolproof is still vulnerable to the password reuse problem and needs physical contacts to ensure that account setup is secure. In [8], J.McCune, A. Perrig, and M. Reiter, proposed a protocol named Bump In Ether. In this protocol, User input traverses a trusted tunnel from the input device to the application .The mobile device verifies the integrity of the host platform and application provides a trusted display through which the user selects the application to which her inputs should be directed, and encrypts those inputs so that only the expected application can decrypt them. Bump in the ether (BitE) is based on TPM. To ensure trustworthy computing on kiosks, invent another system leveraging by TPM and virtual machine (VM) technologies.
In [10], M. Mannan and P. van Oorschot, proposed a MP-Auth protocol (Mobile Password Authentication).In this

Licensed Under Creative Commons Attribution CC BY

protocol long term password is entered through personal device such as cell phone. The personal device provides a user's long-term secrets to a client PC only after encrypting the secrets using a pre-installed, "correct" public key of a remote service (the intended recipient of the secrets). The proposed protocol (MP-Auth) is intended to safeguard passwords from key loggers, other malware (including root kits), and phishing attacks. In spite of that, MP-Auth suffers from password reuse vulnerability. An attacker can compromise a weak server, e.g., a server without security patches, to obtain a victim's password and exploit it to gain his access rights of different websites. On the other hand, MP-Auth assumes that account and password setup is secure. Users should setup an account and password via physical contact, such as banks requiring users to initialize their account personally or send passwords though postal service.

In [12],C. Yue and H. Wang proposed Session Magnifier, a simple approach to secure and convenient kiosk browsing. The key idea of Session Magnifier is to enable an extended browser on a mobile device and a regular browser on a public computer to collaboratively secure a web session. Session Magnifier separates user access to sensitive interactions (online banking or payment) from regular interactions (web surfing or photo viewing). For sensitive interactions, the content is sent to the extended browser on the user's mobile device for further confirmation from a user.

3. Proposed System

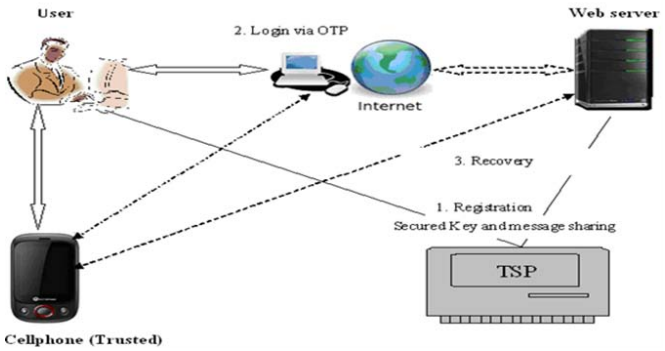


Figure 1: Architecture of proposed system

In the proposed system, a user authentication protocol named oPass which leverages a user's cellphone and short message service (SMS) to prevent password stealing and password reuse attacks. OPass includes cellphone, a browser on the kiosk, and a web server that user wishes to access. Cellphone and the web server interacts through the SMS channel. The web browser interacts with the web server via the Internet. Here, the cellphone interacts directly with the system.

3.1 OPass

OPass consists of registration, login, and recovery phase.

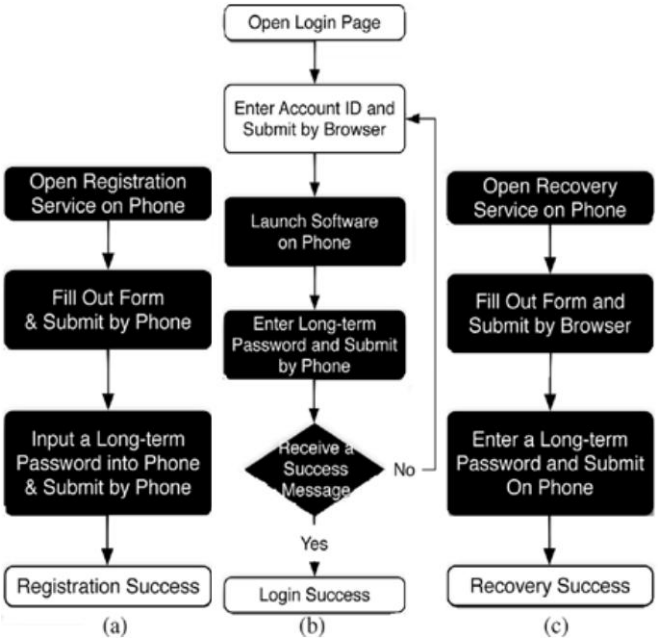


Figure 2: Operation flows for user in each phase of OPass system respectively. Black rectangles indicate extra steps contrasted with the generic authentication system:
(a) registration, (b) login, and (c) recovery.

Above figure explains the operation flow of OPass during each phase. OPass make use of a user's cellphone as an authentication symbol and SMS as a secure network. During login procedure, Opass does not involve users to enter passwords into an untrusted web browser. User name is simply entered into the browser. Now, the user will open the OPass on mobile phone and enter the long term password , OPass will generate a one-time password and direct a login SMS firmly to the server. The login SMS is encrypted by the one-time password. Finally, the cellphone receives a reaction note from the server and shows a victory message on her screen if the server is able to verify her identity. The message is used to ensure that the website is a legal website, and not a phishing one.

3.2 Registration phase

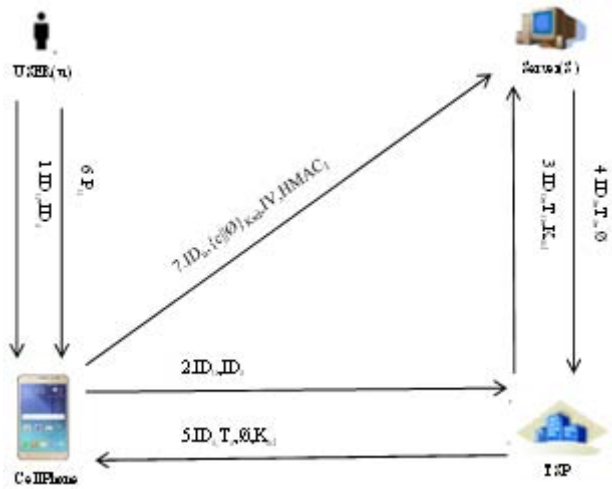


Figure 3: Registration Phase

This phase allows user and a server to exchange a shared secret to authenticate successive logins for this user. The

Licensed Under Creative Commons Attribution CC BY

user will open the OPass program installed on her mobile phone. She enters her account id IDu and server id IDs to the program. OPass sends IDu and IDs to the telecommunication service provider (TSP) through a 3G connection to make a registration request. After receiving IDu and IDs, TSP will trace the user's phone number Tu based on user's SIM card. The TSP will play the role of third-party to distribute a shared key Ksd between the user and the server. Registration SMS is encrypted by using the shared key Ksd with AES-CBC. SSL tunnel is established between TSP and Server S to keep the communication safe. TSP will forward IDu, Tu, and Ksd to the assigned server S. Corresponding information for this account is generated by Server S and will give a response that will include server's identity IDs, a random seed ϕ, and server's phone number Ts. TSP will forward IDs, ϕ, Ts, and a shared key Ksd to the user's mobile phone. Now user will continue to setup the long-term password Pu on her mobile phone. Cellphone computes a secret credential by the following operation:

$$c=H(Pu||IDs||\phi) \quad (1)$$

The cellphone will encrypt the computed credential c with the key and generates the corresponding MAC, i.e., HMAC1. User's identity, cipher text, and IV are given as input to HMAC-SHA1 to produce the output MAC. Cellphone sends an encrypted registration SMS to the server by phone number Ts as follows:

$$\text{Cellphone} \xrightarrow{\text{sms}} \text{Server S: IDu}, \{c||\phi\}Ksd, IV, HMAC1 \quad (2)$$

Server S can decrypt and verify the authenticity of the registration SMS and then obtain c with the shared key Ksd. Server S will compare the source of received SMS with Tu to thwart SMS spoofing attacks. The mobile phone stores the information {IDs, Ts , ϕ, i}, except the long term password Pu and the secret c. Variable i indicates the current index of the one-time password and is initially set to 0. With i, the server can easily authenticate the users mobile phone during each login. After receiving the message, the server stores {IDu, Tu, c, ϕ, i} and then completes the registration [13].

3.3 Login Phase

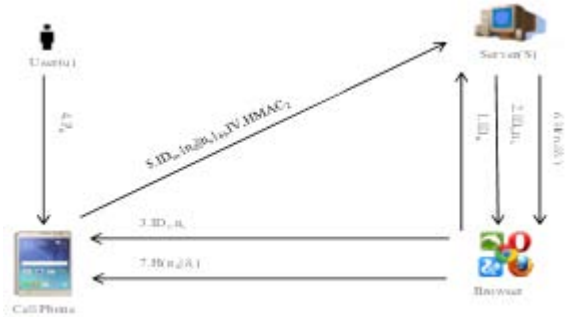


Figure 4: Login Phase

User sends a request to the server S through an untrusted browser on a kiosk. The user uses her mobile phone to generate a one-time password, e.g., δi, and will deliver necessary information encrypted with δi to server S through an SMS message. Depending on the preshared secret credential c, server S will verify and authenticate the user based on δi . The protocol starts when user u wants to log into her favorite web server (already registered).User u begins the login process by accessing the preferred website via a browser on a kiosk. The browser will send a request to Server S with users's account id IDu. Server S will send the IDs and a fresh nonce ns to the browser. Cellphone will receive the same message through bluetooth or wireless interfaces. After receiving the message, cellphone checks the related information from its database via IDs, which will includes server's phone number Ts and other parameters{ϕ,i}. The next promoting a dialog to enter the long-term password Pu will appear on screen of mobile phone. Secret shared credential c can be regenerated by entering the correct Pu on the mobile phone. The one-time password δi for current login is calculated using the following operations:

$$c=H(Pu||IDs||\phi) \quad (3)$$

$$\delta i=H^{N-i}(c) \quad (4)$$

δi is only used for this login and is regarded as a secret key with AES-CBC.A fresh nonce nd is generated by mobile phone . nonce nd and ns are encrypted with δi by the cellphone and it will generate the corresponding MAC, i.e., HMAC2.Server S will receive the following message from cellphone:

$$\text{Cellphone} \xrightarrow{\text{sms}} \text{Server S: IDu}, \{nd||ns\}\delta i, IV, HMAC2. \quad (5)$$

Now, the server recomputes δi(i.e., $\delta i=H^{N-i}(c)$) to decrypt and verify the authenticity of the login SMS. If both the received ns and the previously generated ns are same, then user is a valid else request is rejected. After successful authentication, the users mobile phone will get the success note through the internet. The cellphone will check the received message to confirm the completion of the login process. The phishing attacks and the man-in-the-middle attacks are prevented by this last verification step. If the verification fails, the user will know about the failure of login, and the device would not increment the index i. If the user is successfully log into the server, index will automatically increment, i=i+1, in both the device and the server for one-time password synchronization. After N-1 rounds, One-time password is refresh by recovery phase when user and server will reset their random seed.

Licensed Under Creative Commons Attribution CC BY

3.5 Recovery Phase

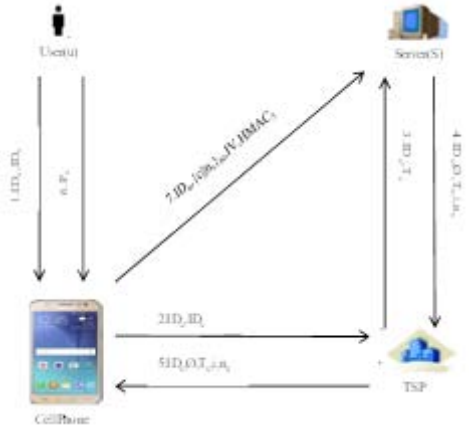


Figure 5: Recovery Phase

Recovery phase is designed for some particular situations; for example, a user may lose her mobile phone. The protocol allows user to recover OPass on her new cellphone assuming she still uses the same phone number (apply a new SIM card with old phone number)[13].First the user will install OPass program on her new cellphone, the program sends a recovery request with her account ID_u and requested server IDs to predefined TSP through a 3G connection. IDs is the domain name or URL link of server. TSP will trace her phone number Tu based on her SIM card and forwards IDu and Tu to server through an SSL tunnel. After receiving the request, server inquiries the account information in its database to check whether the account is registered or not. If account IDu exists, the figures used to calculate the top-secret credential c will be fetched and be sent back to the user. The server generates a fresh nonce ns and replies a message which consists of IDs, ϕ, Ts, i, and ns. This message includes all necessary elements required for generating the next one-time passwords. When the mobile program receives the message, it will ask user to enter her long-term password to reproduce the correct one-time password δi+1.The secret credential c and server nonce ns are encrypted to a ciphertext by users mobile phone. The recovery SMS message is conveyed back to the server for inspection. In the same way, the server computes δi+1 and decrypts this message to ensure that user is already recovered. Now, users new mobile phone is recovered and prepared for future logins. One-time password δi+2 will be used for next login.

4. Experimental Results

We have created an application of OPass. It is a Client-Server model. OPass consist of four entities: User, Browser, Server and TSP. These four entities are divided onto two systems: (User, Browser) acts as Client and (Server, TSP) acts as Server. We have developed a Web server named http://www.eBanking.com. After each and every Login OTP is generated and this OTP goes directly to our http://www.eBanking.com and Home page appears.

All experiments were performed with the configurations Intel(R) Core(TM)i3-4005U CPU @1.70GHz, 4 GB RAM, and the operating system platform is Microsoft Windows 7 Ultimate.



Figure 6: Operator will fill the details



Figure 7: Operator is an authenticated user



Figure 8: OPass program



Figure 9: OTP is generated.

Licensed Under Creative Commons Attribution CC BY



Figure 10: Access Granted



Figure 11: Recovery Phase

5. Conclusion

OPass is an user authentication protocol which influences cell phone and SMS to prevent password theft and password reuse attacks. OPass assumes that each webserver owns a distinctive phone number. Also telecommunication service provider participates in the registration and recovery phases. The principle of OPass is to eradicate the adverse impact of human issues as much as possible. Through OPass, user needs to recall a long-term password which is used to guard their mobile phone. Users are restricted from entering any passwords into untrusted systems for login on all websites. OPass is the user authentication protocol to expect password stealing (i.e., phishing, key logger, and malware) and password apply attacks at the same time. OPass adopts one-time password approach to mark sure individuality between every login. To make OPass fully handy, password regaining is also measured and maintained when users misplace their mobile phones. Users can recover OPass program with re-released SIM cards and long-term passwords. Therefore, we believe OPass is acceptable and reliable for users.

References

[1] M.Wu, S. Garfinkel, and R. Miller, "Secure web authentication with mobile phones," in DIMACS Workshop Usable Privacy and Security Software, 2004.
[2] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," Communication XXXXVII(4), pp. 75–78, 2004.
[3] J. A. Halderman, B. Waters, and E. W. Felten, "A convenient method for securely managing passwords," In Proceedings of the 14th International Conference on World Wide Web,pp. 471–479,2005.
[4] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell, "Stronger password authentication using browser extensions," In Proceedings of the 14th Conference Usenix, Security pp. 2–2, 2005.
[5] K.-P. Yee and K. Sitaker, "Passpet: Convenient password management and phishing protection," In Proceedings of the second Symposium on Usable Privacy Security, pp. 32–43, 2006.
[6] S. GAW and E. W. Felten, "Password management strategies for online accounts," In Proceedings of the second Symposium on Usable Privacy and Security, pp. 44–55, 2006.
[7] B. Parno, "Phoolproof phishing prevention ," in Financial Cryptography and Data Security, C. Kuo, and A. Perrig, springer-Berlin Heidelberg, New York,2006.
[8] J.McCune, A. Perrig, and M. Reiter, "Bump in the ether: A framework for securing sensitive user input," I n USENIX Annual Technical Conference,pp. 185–198,2006.
[9] N. Provos, D. Mcnamee, P. Mavrommatis, K. Wang, and N. Modadugu, "The ghost in the browser: Analysis of web-based malware",In Proceedings of the first Conference on Workshop on Hot Topics in Understanding Botnets,pp.4-4,2007.
[10] M. Mannan "Using a personal device to strengthen password authentication from an untrusted computer," in Financial Cryptography Data Security, P. van Oorschot, springer-Berlin Heidelberg, New York,2007.
[11] S. Garriss, R. Cáceres, S. Berger, R. Sailer, L. van Doorn, and X.Zhang, "Trustworthy and personalized computing on public kiosks, "In Proceedings of the sixth International Conference, pp.199–210, 2008.
[12] C. Yue and H. Wang, "Session Magnifier: A simple approach to secure and convenient kiosk browsing," In Proceedings of the eleventh International Conference Ubiquitous Computing, pp. 125–134, 2009.
[13] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin (2012), "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks", IEEE transactions on information forensics and security, pp. 651-663, 2012.
[14] Vaishnavi Yalamanchili , Dr.P.Pandarinath," Improved Password Authentication System against Password attacks for web Applications", International Journal of Computer Trends and Technology (IJCTT), IV (8), pp. 2878-2883,2013

Author Profile



Mirza Tanzila Maqsood has received B.E degree in Computer Engineering from Amrutvahini College of Engineering, Sangamner, Pune University in 2009.Now she is pursuing Masters in Engineering(Computer Science and Engineering) from M.S.Bidve Engineering College, Latur, SRTM University Nanded, Maharashtra.



Prof. Shrikant R. Tandale has received B.E De B.E degree in Electronics from SGGS College of Engineering and Technology, Nanded. He has persued his M.E degree in Computer Science and Science and Engineering from MGM college of Engineering. He is working as Assistant Professor and Head of Department of Computer Science and Engineering in M.S Bidve Engineering College since 1990. He is pursuing his research work in Wireless Sensor Networks in Swami Ramanand Teerth Marathwada University, Nanded.

Licensed Under Creative Commons Attribution CC BY