International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 6, June - 2014

An Enhanced Authentication Protocol Resistant to Password Stealing and Reuse Attack

Sharayu A. Aghav
Department of Computer Engineering
MIT College of Engineering
Pune-38, India

Rajneeshkaur R. Bedi
Department of Computer Engineering
MIT College of Engineering
Pune-38, India

***Abstract*— With the fast propagation of time, most of the activities are now available on internet. In this environment, users have to be authenticated before to being granted access to sensitive contents. Password is the predominant tool which protects data and keeps information digitally safe. It is been seen that text password stays popular than the other forms of passwords due to its simplicity and convenience. Therefore, it can be easily stolen and misused under different vulnerabilities such as hacking, identity theft, Cyber stalking and website cloning. Users are likely to choose weak passwords and reuse the password for various websites. In this case if one password is revealed, it can be used for all other websites. This is called as the Domino Effect. Another issue is when a person enters his/her password into an untrusted computer; the adversary can steal password by launching attacks such as phishing, malware and key loggers etc. In this paper, we propose a simple approach which allows a client to counter such attacks by separately entering a long-term secret used to generate one-time password for each login session on all websites through an independent personal trusted device such as a cell phone, which provides two-factor authentication. Along with this, system requires each participating website possesses a user's unique cell phone number and involves telecommunication services in registration and recovery phases.**

Keywords*— Network Security; Password Authentication Protocols; Phishing and Password Reuse Attacks.

I. INTRODUCTION

Today, web browsing has become almost an important part of everyday lives as we perform many activities on internet such as banking, bill-paying and shopping. Hence, user authentication is the most essential part as far as security of sensitive information is concerned. Text password is simple and convenient thus, been adopted as the primary mean of user authentication for websites. But at the same time it faces several problems such as spyware or malware [8], keylogging, phishing [9] and also now a day's computer users need to remind an increasing number of passwords as they join new password protected sites such as e-commerce sites, host accounts, email servers and online financial services over time. Usually, password-based user authentication can resist brute force and dictionary attacks if users select enough strong passwords. Unfortunately, it seems that users are unable to memorize the large number of distinctive, secure passwords for all user accounts and probably remain constant as the number of passwords increases for growing sites. Choosing passwords for increasing number of sites raises a critical issue is that users be likely to reuse passwords across different websites [10], [11]. In 2007, Florencio and Herley [12] specified that a user reuses a password across 3.9 various websites regularly. Password reuse is the reason behind users to lose sensitive information stored in various websites if a hacker suspects one of their passwords. This attack is referred as the password reuse attack. Therefore, passwords are a main target of adversary to get an access to sensitive information which makes it as a favorite area of researchers.

In a solution we require Multifactor Authentication techniques to protect web transactions and to raise faith of users on mobile financial transactions. In this paper, an authentication system that is both secure and highly usable based on multifactor authentication approach. It uses a novel approach to establish an authentication system based on a long-term password entered through mobile device used to generate one-time passwords avoids both password stealing and reuse attack and SMS as a secure transmission channel.

The remainder of this paper is organized as follows. In the next section, a brief literature survey on two-factor authentication mechanism variants is described. Section III states problem definition and assumptions for our system. Section IV discusses the proposed solution in detail. Section V provides an analysis of the security of our approach. Section VI summarizes our conclusions providing future direction.

II. RELATED WORK

The internet is wide area network which is inherently insecure. The internet users who perform various activities get affected by security threats such as denial of service attacks, sniffing, spoofing, keylogging, hacking, phishing, virus, worms and various forms of malwares etc. It is necessary that strong security measures should be implemented which can satisfactorily deal with and control security threats. All the websites those allow critical information storage and transfer such as internet banking systems should authenticate users before granting access to particular services. The literature available represents different authentication approaches. The classification of available authentication techniques into four categories based on their different objectives is depicted in the Fig. 1.

Even though there are a variety of authentication protocols in a range from typically more complex and costly, password based authentication is still the most common technique even in such an unsecure environment. The U.S. Federal agencies guidelines [OMB 04-04] categorize four levels of e-authentication as far as the effects of authentication fault and misuse of credentials are concerned as shown in Table I. The more severe the effect of an authentication fault, the higher the level of assurance required.

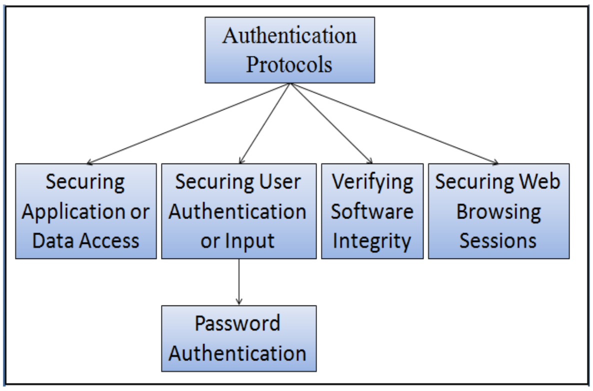
Authentication Protocols
Securing Application or Data Access
Securing User Authentication or Input
Verifying Software Integrity
Securing Web Browsing Sessions
Password Authentication

Fig. 1. Analyzed Classification of Authentication Techniques

The OMB 04-04 gives the criteria to determine the level of e-authentication assurance needed for specific applications and transactions, on the basis of the threats and possibility of occurrence of each application or transaction [13].

TABLE I. AUTHENTICATION LEVELS [13]

Level 1: No identity proofing (little confidence in asserted identity; weak passwords are allowed and is vulnerable to eavesdropping.)
Level 2: Single-factor, using better passwords (some confidence in asserted identity; but still vulnerable to phishing, social engineering and other attacks.)
Level 3: Two-factor, e.g., password and soft crypto token or one-time password device (high confidence in asserted identity; phishing attacks shouldn't get password authentication secrete.)
Level 4: In-person identity proofing, requiring hard crypto tokens and utilizing crypto binding of authentication and data transfer (very high confidence in asserted identity.)

Table II. gives a survey on the use of two-factor mechanism for user authentication on the web. Two-factor mechanism gives simple and convenient way for user authentication. Although variants of two-factor authentication techniques proposed in literature have potential to increase security, experiences some limitations while dealing with communication channel, processing time [1], [2], [3], [4], [5], [16], [17] along with system usability [6], [7]. Hung-Min Sun et al. [1], introduced an oPass user authentication protocol to divide a system between a small trusted mobile device and a bigger, more powerful, but possibly untrusted computer, provides security and high usability as compared with other systems. While dealing with limitations, our solution is inspired by this protocol which gives rise to the integrated architecture for online authentication.

Our Contribution:

1) We do not split a TSP proxy from server rather integrate TSP module with server incurs dropping of SSL channel between them which causes to avoid possible threats.
2) Integration causes to reduce communication overhead in the system.
3) Merging inevitably causes reduction in cost of system.

III. PROBLEM DEFINITION AND ASSUMPTIONS

An approach involves user accomplishes secure login to the web server by directly operating a cellphone and browser on an untrusted computer. A long-term password entered through a cellphone used to compute one-time password for each session. The communication between the cellphone and the web server is through SMS channel, transmits authentication messages. The assumptions in system are as follows.

1) Every web server holds a unique phone number. Via SMS channel, users can access each website using a unique phone number.

2) The telecommunication service provider plays an essential role in the registration and recovery phases. The TSP module acts as a communication bridge between subscribers and a web server. It helps subscriber by offering a service to perform the registration and recovery process with each web service e.g., a subscriber inputs her id and a web server's id in the application to execute the registration phase. Afterwards, the TSP module sends the registration request and the subscriber's phone number to the web server based on the received server's id.

3) Subscriber's (i.e., users) communication with the server integrated TSP module through 3G connection.

4) If a user loses his cell phone, he can inform service provider (TSP) to disable misplaced SIM card and get a new card with the same phone number to successfully finish the recovery phase.

IV. PROPOSED SCHEME

This section describes system overview from the user perspective. System consists of *registration*, *login*, and *recovery* phases. Further, each phase explained in detail.

A. System Overview

Overview followed from [1]. Contrasting with general web logins, system makes use of a user's cell phone as an authentication token and SMS as a secure communicating medium. User starts with the registration phase, a user go on to launch the program to register his new account on the website, she desires to access later. On contrary to conventional registration, the server asks for the user's account id and phone number, in spite of password. After filling out the registration form, the program requests the user to enter a long-term password. A long-term password generates a chain of one-time passwords for next login sessions on a target server. Afterwards, by default the program sends a registration SMS to the server to complete the registration procedure. The registration SMS is encrypted to provide data confidentiality. Contrasting with common cases, login process in system does not require users to type passwords into an untrusted web browser. Simply, the user name is the only input information to the browser. After that the user starts the program on her phone and enters the long-term password; the program will produce a one-time password and sends a login SMS encrypted by the one-time password safely to the server. At last, the cell phone receives a response message from the web server and shows a success message on his screen if the server is able to confirm his identity. The message guarantees that the website is an authorized website and not a phishing one. A *recovery* phase helps to fix problems in circumstances, such as losing one's cellphone.

TABLE II. COMPARATIVE ANALYSIS OF TWO-FACTOR AUTHENTICATION VARIANTS

TPM STANDS FOR TRUSTED PLATFORM MODULE

Category based on Objective	Purpose	Techniques	Advantages	Disadvantages
Securing User Authentication or Input	Password Stealing and Password Reuse Prevention.	One-time passwords. A SMS service. A TSP as a proxy. (Browser on an untrusted computer, oPass program on mobile device.)[1]	1. Our system requires only the URL of site and their username. 2. Free users from having to remember or type any passwords into conventional computers for authentication.	1. Attacker may compromise the session key of SSL tunnel. 2. Attacker may compromise the session key of 3G connection.
		A pre-shared secret. An encryption table. A proxy. A key pair (public and private keys). (Browser on an untrusted computer.)[2]	1. Minimize user input: System requires only the URL of site and their username.	1. Compromization of key by Key Exhaustion in the encryption table. 2. Proxy may get compromised.
		One-time passwords. Transaction Passwords. A SMS service. A key pair (public and private keys). (Browser on an untrusted computer.) [16]	1. Provides the transaction integrity.	1. Users provide pin number into website on conventional computer. 2. Additional work of computing transaction password.
		TIC (Transaction Identification code) Authentication. A SMS Service. (Browser on an untrusted computer.) [17]	1. System provides secure environment that does not require any change in traditional infrastructure.	1. Users provide password into website on conventional computer. 2. Attacker may compromise TIC codes stored into mobile device.
	Password Stealing Prevention.	A bank's public key. A key pair (public and private keys). (Browser on an untrusted computer.)[3]	1. Provides the transaction integrity.	1. Attacker may eavesdrop bank's public key available in mobile device.
		A pre-shared secret. A key pair (public and private keys). (Browser on a mobile device.)[4]	1. Avoid dependence on the untrusted computer's browser's interface.	1. Attacker may hijack (user) public key re-establishment process. 2. Non- technical users may face problem.
		A trusted proxy. A key pair (public and private keys). (Browser on an untrusted computer.)[5]	1. Minimize user input: Our system requires only the URL of the proxy and their username. 2. Make the system's security-relevant decisions visible to the user; give the user the ability to override the system's actions.	1. Proxy may get compromised. 2. Attacker may compromise the session key of SSL tunnel.
		TPM based system The public Attestation Identity Key (AIK). A key pair (public and private keys). A symmetric key. An encrypted tunnel. (Application on an untrusted computer.)[6]	1. BitE is feasible on commodity hardware. 2. BitE offers some protection for legacy applications. 3. Operation of BitE is convenient and intuitive for users.	1. Compromise of Active Application causes buffer overflow attack. 2. Compromise of Active Kernel on Host Platform causes attacker to capture sensitive user input despite the BitE system.
		TPM based system The public Attestation Identity Key (AIK) certificate. A key pair (public and private keys). (Application on an untrusted computer.)[7]	1. Increases trustworthiness of kiosk without compromising it's functionality	1. Run time software attack possible. 2. Physical security breach –Hardware attacks. 3. Physical access incurs Barcode attacks.

B. Registrtion Phase

Fig. 2 describes registration phase. This phase intends to allow a user and a server to consent on a shared secret to authenticate user for subsequent logins. The user starts the program on his cell phone. He inputs ID_u (account id) and ID_s (generally the website URL or domain name) to the program. The mobile application then forwards ID_u and ID_s to the telecommunication service provider (TSP) which is integrated with a web server only; through a 3G connection to make a registration request. The TSP module received the ID_u and the ID_s, it is able to trace the user's phone number T_u based on user's SIM card. The TSP module acts as the third-party to share out a shared secrete key K_{sd} between the user and the server. The shared secrete key encrypts the registration message (SMS) with AES-CBC encryption algorithm. Then the TSP sends ID_u, T_u and K_{sd} to the related server by functional call. Server will form the related information for this particular account and reply to the TSP module with a response, containing server's identity ID_s, a random seed $\emptyset$ and server's phone number T_s. The TSP module then sends ID_s,T_s, $\emptyset$ and a shared secrete key K_{sd} to the cellphone. After successful reception of the response, the user can provide a long-term password P_u through his cellphone.

The operation below describes the method to calculate a secret credential c by the cellphone:

$$c = H(P_u \| \mathrm{ID}_s \| \emptyset). \tag{1}$$

The cell phone produces cipher text by encrypting the computed credential c with the key K_{sd} and forms the corresponding MAC, i.e., HMAC. HMAC-SHA1 obtains input user's identity, cipher text and IV to output the MAC [14], [15] and sends this as a secure registration SMS. The encrypted registration SMS to the server by phone number T_s as follows:

$$\text{Cellphone} \xrightarrow{SMS} Server\left(\mathrm{ID}_u, \{c \| \emptyset\}_{K_{sd}}, IV, \mathrm{HMACSHA}_1\right). \tag{2}$$

The server checks the authenticity of the registration SMS by decrypting it with the shared secrete key K_{sd} and required information is obtained.

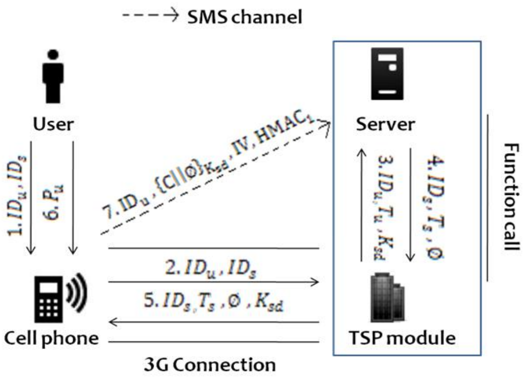

Fig. 2. Process of Registration Phase

To avoid SMS spoofing attacks, server checks the source of received SMS with T_u . At the end, the cell phone stores all information $\{\mathrm{ID}_s, T_s, \emptyset, i\}$ excluding for the long-term password P_u and the secret c . The current index of the one-time password is specified by variable i and is initialized to 0. The server authenticates the user device during each login with i. After receiving the long-term password, the server stores $\{\mathrm{ID}_u, T_u, c, \emptyset, i\}$ and finishes the registration phase.

C. Login Phase

Fig. 3 shows the detail flow of the login phase. The user starts by sending login request to the server through an untrusted browser (on a kiosk) with his account ID_u. In the response server supplies the ID_s and fresh nonce n_s to the browser. At the same time this message is forwarded to the cellphone through Wireless or Bluetooth interfaces. On the reception of the message, the cell phone checks related information in its database via ID_swhich encompasses server's phone number T_s and other parameters $\{\emptyset, i\}$. After proper checking, it asks user to enter a long-term password P_u . The program on the cellphone generates secrete shared credential c for a correct long- term password P_u . The operation below is used to recalculate a one-time password δ_i for current login:

$$c = H(P_u \| \mathrm{ID}_s \| \emptyset). \tag{3}$$

$$\delta_i = H^{N-i}(c). \tag{4}$$

δ_i is only used for this login (ith login after user registered) and as a secret key with AES-CBC for encryption. The cell phone produces a fresh nonce n_d and encrypts n_d and n_s with δ_i to generate the related MAC, i.e., HMAC and forms a secure login SMS which is then sent to server S as below:

$$\text{Cellphone} \xrightarrow{SMS} Server\left(\mathrm{ID}_u, \{n_d \| n_s\}_{\delta_i}, IV, \mathrm{HMACSHA}_2\right). \tag{5}$$

The server recomputes δ_i (i.e.,$\delta_i = H^{N-i}(c)$) after receiving the login SMS to confirm the authenticity of the login SMS and check required information by decrypting it. If the nonce n_s received equals the prior generated nonce n_s, the user is

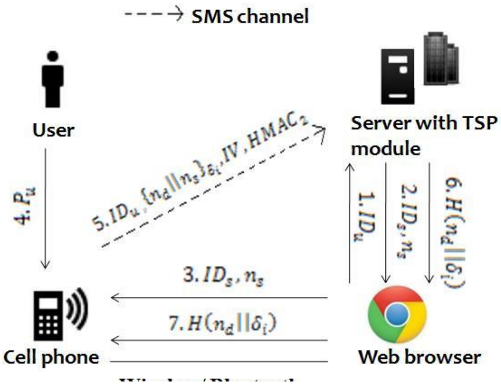

Fig. 3. Process of Login Phase

valid one; else, the server will reject the login request.

The server sends a success message $H(n_d||\delta_i)$ to the user's cell phone by successfully verifying user's identity. The cell phone checks the received message to finish the login procedure. The last verification avoids the phishing attacks and the man-in-the-middle attacks. If verification fails, the user knows a reason and the device would not increment the index i. After successful user login, index will automatically increase, $i = i + 1$ concurrently in both the device and the server for synchronization of one-time password. With the recovery phase one-time password can be refreshed, user and the server can reset random seed $\emptyset$ after specific period, $N - 1$ rounds (where N is pre-defined length of hash chain).

D. *Recovery Phase*

Fig. 4 shows the detail flow of the recovery phase. Recovery phase is significant, helps in maintenance of the system by providing a way to regain a system in some circumstances (e.g., a user lost his cellphone or a SIM card.). The system can be recovered on users' new cell phone (a new SIM card with old phone number (Number portability)). When user installs the program on his new cell phone and starts the program, user asks for a recovery with same previous account id ID_u and requested server ID_s to TSP module through a 3G connection. As we declared earlier that ID_s can be the domain name or URL link of server. Same in the registration process, TSP module can trace user's phone number T_u based on his SIM card and sends user's account id ID_u and T_u to server through a functional call. On reception of the request, server looks for the account information in its database to verify whether account already exists or not. If account ID_u already exists then the information used to calculate the secret credential will be extracted and be returned to the user. The server produces fresh nonce n_s and replies with a message which contains ID_s,$\emptyset$,T_s, i and n_s i.e., all the required parameters to produce the next one-time passwords to the user for each login session on all the websites.

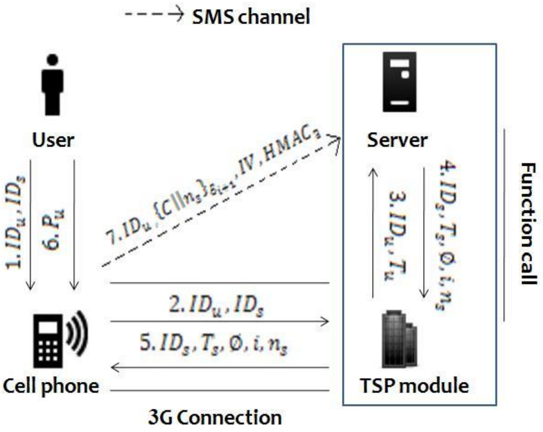
SMS channel
User
Server
Cell phone
TSP module
3G Connection
Function call
1. ID_u, ID_s
6. P_u
7. ID_u, $\{C||n_s\}_{\delta_{i-1}}$, IV, $HMAC_3$
2. ID_u, ID_s
5. ID_s, T_s, $\emptyset$, i, n_s
3. ID_u, T_u
4. ID_s, T_s, $\emptyset$, i, n_s

Fig. 4. Process of Recovery Phase

Same as the registration process, when the mobile application receives the message; it asks the user to enter his long-term password to regenerate the correct one-time password δ_{i+1} (presuming the last successful login before user lost his cell phone is δ_i). At last, the user's cellphone produces a cipher text by encrypting the secret credential c and server nonce n_s and return it back as a recovery message to the server for verification. Likewise, the server calculates δ_{i+1} and decrypts this recovery message to confirm that user is already recovered. Now, user's new cell phone is recovered successfully and ready to execute further logins. For the subsequent user login, one-time password δ_{i+2} will be used.

V. SECURITY ANALYSIS

In this section, we analyze the security properties of our solution.

A. *Security Properties*

Here, we discuss various attacks that can be launched on password protocols. This list covers all the password attacks that appeared on previous literatures. We show that our system is secure against each of them.

1. *Eavesdropping attacks*: In this, an attacker snoops the communication between a client and a server to discover the client's password. Since in this system, client communicates with server through an out-of-band SMS channel that protects the exchange of messages between users and servers. An eavesdropper cannot discover the client's password due to the use of a one-time password technique.
2. *Message replay attacks*: In this type of attack, an attacker first eavesdrops the communication between a client and a server, then attempts to login on the server by replaying some messages that the attacker captured previously. System is safe against message replay attacks as system messages are encrypted by one-time password in different runs of system. Second, system itself is secure against message replay attacks. If an attacker eavesdropped a user's login SMS, he can masquerade the user to deliver the same login messages to the web server. However, login will fail, because the stolen login SMS has already been used for login. Note that the message verification information stored in the server is modified if and only if the message from the client is successfully verified.
3. *Message log compromise attacks*: This type of attack an attacker steals the message log file, which stores all the messages exchanged between a client and a server. In addition, these messages are not encrypted by the secrete key established by a client and server or one-time password. This is a strong attack since we assume that the attacker could get all the messages of past sessions in plain text. However, system is secure against this type of attack for the following two reasons:

   a) Messages cannot be reused: In system, each message is unique, non predictable and each message can only be used once. Hence, an attacker cannot reuse any of the messages to gain unauthorized access.

a) Password cannot be computed: Similarly, it is not computationally feasible to obtain the password P from the message in the form of $HMACSHA$ or the user message information $ID_u, T_u, C, \emptyset, i$. Note that the user message information stored in the server gets modified if and only if the message from the user is successfully verified i.e., at the time of successful registration or login only and any message is used for once. Therefore, knowing old message does not enable an attacker to be able to modify the message verification information in the server.

4. *Phishing Attack*: In this type of attack, the attacker launches attack to impersonate itself as a valid user without getting noticed. Since in this protocol, users input account ids into the kiosk and enter their long-term password into the cellphone. System adopts one-time password δ_i generated from long-term password used for each login session on all the websites, also treated as a secret key for encryption and is never transmitted hence, prevents against password reuse attack. The attacker also cannot recover the δ_i from the encrypted login SMS. Hence, phishing attacks do not work.
5. *Spoofing Attack*: The server compares the source of received registration SMS with previously registered user phone number T_u to prevent SMS spoofing attacks.
6. *Also, this* protocol prevents from Man-in-the-middle attack, Brute force attack, Server spoofing attacks, Online dictionary attacks, Off-line dictionary attacks, Keylogging, Session hijacking.
7.

VI. CONCLUSION AND FUTURE SCOPE

The different aspects of Password based User Authentication, Level-wise Password based Authentication Techniques and Applicability of those techniques for User Authentication are studied and analyzed, which facilitate discovering the scope of research for Password based User Authentication Mechanism when dealing with possible attacks on the system. This idea motivated to propose a novel architecture for user authentication avoids most possible threats to achieve higher security of the system. Hence, the proposed technique is believed to defeat attacks possible due to the communication link i.e. SSL connection and other techniques studied in the literature.

The proposed system uses the concept of two-factor authentication, one-time password and telecommunication service along with web services to accomplish improved security. Since, no system is free from drawbacks; the future work is towards handling this issue along with improvement in performance of system further implement a user authentication system works on multiple parameters to authenticate user e.g., three-factor authentication (Biometric).

REFERENCES

[1] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin. (2012, April.). oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks. *IEEE Transactions on Information Forensics and Security*. 7 (2).

[2] D. Florencio and C. Herley. Klassp: Entering passwords on a spyware infected machine using a shared-secret proxy. In Proc. of the ACSAC, 2006.

[3] M. Mannan and P. van Oorschot, "Using a personal device to strengthen password authentication from an untrusted computer," in *Proc. Financial Cryptography Data Security **2007***, pp. 88–103.

[4] B. Parno, C. Kuo, and A. Perrig, "Phoolproof phishing prevention," in *Proc. Financial Cryptography Data Security 2006*, pp. 1–19.

[5] M.Wu, S. Garfinkel, and R. Miller, "Secure web authentication with mobile phones," in *DIMACS Workshop Usable Privacy Security Software*, 2004.

[6] J.McCune, A. Perrig, and M. Reiter, "Bump in the ether: A framework for securing sensitive user input," in *Proc. USENIX Annu. Tech. Conf.*, 2006, pp. 185–198.

[7] S. Garriss, R. Cáceres, S. Berger, R. Sailer, L. van Doorn, and X. Zhang, "Trustworthy and personalized computing on public kiosks," in *Proc. ACM 6th Int. Conf. Mobile Systems, Applications Services*, 2008, pp. 199–210.

[8] A. Moshchuk, T. Bragin, S. D. Gribble, and H. Levy, "A crawler-based study of spyware in the web," in *Proc. Symp. Network and Distributed System Security (NDSS)*, 2006.

[9] Anti-Phishing Working Group. Phishing Activity Trends Report, July, 2006.

[10] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Commun. ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[11] S. Gawand, and E. W. Felten, "Password management strategies for online accounts," in *Proc. SOUPS '06: ACM 2nd Symp. Usable Privacy. Security*, pp. 44–55.

[12] D. Florencio, and C. Herley, "A large-scale study of web password habits," in *Proc. WWW '07: ACM 16th Int. Conf. World Wide Web*, 2007, pp. 657–666.

[13] Assad Moini and Azad M. Madni. (2009, December.). Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective. *IEEE Systems Journal*. 3(4).

[14] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," in *Proc. Advances Cryptology—ASIACRYPT 2000*, 2000, pp. 531–545.

[15] H. Krawczyk, "The order of encryption and authentication for protecting communications (or: How secure is SSL?)," in *Proc. Advances Cryptology—CRYPTO 2001*, 2001, pp. 310–331.

[16] Safa Hamdare, Varsha Nagpurkar, and Jayashri Mittal, "Securing SMS Based One Time Password Technique from Man in the Middle Attack," *International Journal of Engineering Trends and Technology*, May. 2014, vol. 11, no. 3, pp. 154-158.

[17] Ayu Tiwari, Sudip Sanyal, Ajith Abraham, Svein Johan Knapskog, Sugata Sanyal, "A Multi-Factor Security Protocol For Wireless Payment-Secure Web Authentication Using Mobile Devices," *Proc. IADIS International Conference Applied Computing, 2007, pp. 160–167*.