Personal Secret Information Based Authentication towards Preventing Phishing Attacks

Gaurav Varshney, Ramesh Chandra Joshi, and Anjali Sardana

Electronics and Computer Engineering Department, Indian Institute of Technology,
Roorkee, India
{gauravdtsi,rcjosfec,dr.anjalisardana}@gmail.com

Abstract. Phishing is a well-known technique used by internet fraudsters for acquiring sensitive and personal information from users by impersonating a real identity. A Phishing attack involves various deceptions & advanced cybercrime techniques, some of them includes email spoofing, exploiting browser side vulnerabilities, fraudulent emails and Phished websites creation techniques using scripting languages and technologies. Phishing causes identity, goodwill and money loss to companies and individuals. One of the major problems we identified is the reduced usage and reliability on the email Infrastructure as a communication medium between customers and companies. Previous schemes for phishing prevention such as those which use browser extension, Quick Response code, Extended Authentication server & device and smart card based techniques are complex and difficult to make use in real world scenario. We present an architecture that can be used by companies for preventing phishing attacks by sharing a piece of secret information with every customer and using it as an authentication mechanism to prove their originality when a customer login to their websites using links provided in their emails. The unavailability of secret information which is securely shared between customer and the company will prevent a phisher in creating deception and hence will prevent phishing attacks which occur due to malicious links in phished emails. This will increase the reliability of email service as an authentic communication medium. The efficacy of this technique does not rely on results of any spam or phishing prevention scheme provided at email service provider side.

Keywords: Phishing, phisher, authentication.

1 Introduction

Phishing was known to people in the year 1996. It can be defined as an art of deceiving people on the internet, so as to steal the personal information secret to them such as user names, passwords, bank account numbers, credit card details etc. The concept was termed as phishing as the fraudsters are using emails as a medium to “Phish” user information such as usernames and passwords in the sea of internet users. The name resembles the word fishing; ‘ph’ is used instead of ‘f’ for two reasons:

N. Meghanathan et al. (Eds.): Advances in Computing & Inform. Technology, AISC 176, pp. 31–42.
springerlink.com

1. To make it a different word
2. The letter ‘ph’ is derived from the word “phreaking” which is known to be the earliest form of hacking of telephone lines.

Phishing come first time into the knowledge of people as a severe attack in 1996 when cyber criminals stole American Online Passwords by deceiving the AOL users through phishing [11].

Phishing is a deception technique used by attackers (Commonly known as Phishers) for gaining personal information from end users, with the help of fraudulent and spoofed emails, Phished Websites and various deception techniques. The aim of the phisher lies in obtaining personal information or credentials from an end user such as bank account numbers their passwords, credit card details etc. They use this information in doing mischievous and fraudulent activities such as accessing important information and secrets, withdrawing money of an individual on web.

Phishing starts when an attacker uses a mass-mailer for sending fraudulent and spoofed emails by impersonating themselves as an authenticated bank, financial or social institution to a large population of end users. Phishing generally starts with a mass mailing activity to increase the population of end users that will eventually fall for Phishing. Phishers also use a phished website that looks exactly same as that of the original one he is targeting to phish, except for the domain name and the DNS entry it will use. The attack scenario starts when the attacker sends a phished email using spoofing and advanced email creation techniques such as those used in email newsletters, with other fraudulent techniques to fulfill their specific needs. The end user or the victim opens the email and because of deception techniques used inside it, trusts on the originality of its contents and its sender and clicks on the URL specified in it. The URL looks normal but it will take to a phished Web site.

The phished website is created in a way to look like an original highly trusted site that a phisher is targeting. As an example a phishing website can be of a highly trusted bank having the same text the same logo and animations as it is on the original bank website. When a user reaches a phished website which he can’t identify as phished one, he enters information asked by the website such as user id’s password, credit card numbers etc. which eventually get stored in the servers of the phisher.

Phishing is termed as a deception technique as it creates an illusion to the receiver of an email that, it is from an entity on which user’s trust, but behind the scenes it is not as expected. Email phishing is carried out with the help of many other tricky techniques which are used for internet fraud in today’s internet world, one of which is Email spoofing. Email spoofing technique allow an attacker to send email using other’s identity which causes a severe problem, because now he can send anything such as wrong information, malicious codes etc. and held others responsible for his wrongdoings. Spoofing creates two problems: one is of creating wrong trust in the mind of end user, hence gaining confidence, so that he will do what is required and second is of wrong backtracking because an innocent user or group will be held responsible for the problems created. Email spoofing plays an important role in carrying out email phishing as it makes the user to believe on the illusion of reality, created by a Phisher.

The statistics as obtained from Avira shown in Table 1. are of February 2011 which shows that phishing attacks are more Top level domain and business centric. The most phishing attacks are on the .com top level domain and the companies which gets most affected are those which involve some kind of electronic money transfers and social networking. Hence Phishing is from one of the most important threats in the internet world that is to be taken care of. The damages that it causes include loss of money, information and good will.

Table 1. Statistics of Phishing Attacks

#	Top Level Domain	%	#	Brand Name	%
1	.com	51.56	1	PayPal	53.59
2	Others	15.82	2	Others	20.03
3	.org	6.20	3	HSBC Bank	5.07
4	.net	5.94	4	Chase Bank	4.43
5	.uk	3.69	5	Facebook	4.09
6	IP address	3.22	6	EBay	3.48
7	.br	2.44	7	Bank Of America	3.16
8	.tk	2.18	8	Visa	2.19
9	.ru	2.01	9	Lloyds	2.07
10	.tl	1.23	10	Banco Satander	1.88

In this paper we propose an architecture that will solve the problem of phishing that is launched through Phished website links in emails. The problem created by this attack is of bad trust in email service as an authentic communication medium and loss of credentials of users.

The next section will describe the previous schemes for phishing prevention. Section 3 will describe our proposed scheme with section 4 giving the description of overall benefits. Section 5 ends the discussion with conclusions and future work.

2 Previous Work

A detailed description of previous schemes proposed for preventing phishing attacks with their assumptions, advantages and disadvantages are in a Table shown on the next page. From the study of previous techniques we concluded that there are some common shortcomings in them which are as follows:

1. Various Schemes based on Secret Images shared between website and user and which are revealed during pre-logging when the user enters the secret key are annoying and vulnerable. As they ask users to enter a new watermark image and its position each time a user logs out, also a Phisher can obtain the secret key from the user by creating fake login pages and can obtain the Watermark image and its location from the original web page by using the secret key obtained from the user.
2. Use of Advanced Technologies such as Radio frequency Identification Technology (RFID) for authentication requires that a user must carry the RFID reader and Tokens for Login.

3. External authenticating device usage in prevention of phishing attacks add on to the cost and complexity. Complexity is increased because the user interaction will be secure but complex as now it requires external device communicating with the browser which will then eventually contact to the target server. Also it will always require an external device for secure access.
4. Those solutions that require client server support require changes in the underlying frameworks and architectures also their maintenance and proper synchronization is a requirement. Also real time implementation, deployment and performance are of great concern.
5. Email Authentication and verification schemes require key management activities which will increase an extra burden on the system as now system has to take care of keys for each and every user.
6. Techniques implemented for avoiding key logging and improving password schemes are complex with respect to a normal user as he certainly doesn't want to annoy on every time he logs on to the website by entering keys through keypads and hence require initial user training.
7. Those schemes that implement security of user passwords at client's side with browser extensions are difficult to implement.
8. Client server interaction for authentication during every secure transaction increases the communication and computation cost at both client and server side.
9. Schemes based on short time passwords and certificates require special systems such as offline card readers (FINREAD reader) and Smart cards for their generation which add up extra cost and complexity to the underlying system.

Abbreviation	**Proposed Scheme**	**Paper name**	**Assumptions**	**Advantages**	**Disadvantages**
Watermarking Based [1]	Author proposed an anti-phishing approach based on Dynamic watermarking technique. According to this approach user will be asked for some additional information like watermark image, its fixing position and secret key at the time of user's registration and these credentials of particular user will be changed at per login. During each login phase a user will verify the authentic watermark with its position and decide the authenticity of website.	**Detection and Prevention of Phishing Attack Using Dynamic Watermarking** A.P. Singh et.al **2011**	User will select a watermark image and its position at website while logging out. User Account database that will store secret key & Watermark Image with regular credentials.	Doesn't require any external mobile device. Feasible to implement with minimal changes.	During every logout user is asked for reentering new watermark image and its position which is annoying. A phisher can obtain the initial secret key through phishing and can obtain the watermark position and its location.
RFID Based [2]	Authors proposed a RFID (Radio Frequency Identification Technology) Factor Authentication Application (RFAA) techniques; an enhanced technique from SofToken scheme that acts as a technique for two-factor authentication.	**A Sophisticated RFID Application on Multi-Factor Authentication** J.C. Liou et.al 2011	RFID tags and RFID reader and changed Login Infrastructure.	RFAA is a two factor authentication scheme for more secure identification. RFAA can be used for both online transactions and computer system access as opposed to the SofToken application that primary addresses to online transaction security	RFID reader and Tokens will be required each time user login.

External Authentication Device based [3]	Author proposed techniques based on external authenticator. They proposed that user's must be authenticated by an external authenticator that they cannot reveal to malicious parties. Scheme uses additional authenticator on a trusted device, which can be a cell phone or a PDA, such that the attacker will have to compromise the device to obtain user password and to obtain user account.	**Phool-proof Phishing Prevention** B. Parno et.al 2005	User can establish a secure connection between their cellphone and their browser and the cellphone itself has not been compromised.	Prevent active man in middle attacks. Use of cellphones allows us to minimize the effect of hijacked browser windows and facilitates user convenience since it can be used at multiple machines.	Requires the usage of external authenticating device to solve the purpose which will add complexity in the way a user account will be accessed.
Post Phishing Rescue based [4]	Authors proposed post Phishing Rescue technique. Here client identifies whether user have entered valid credentials on a faked website and Server capture this information from various clients. if there is some phishing going on server transfer the information to target domain for immediate attention.	**Password Rescue: A New Approach to Phishing Prevention** D. Florˆencio and C. Herley 2006	Assuming that white list and a black list are maintained and updated regularly and a notion of trusted client and server ends who will cooperate.	The scheme doesn't protect the user from information leakage but rather try to detect and then rescue the user from bad trust decisions.	Complex and require client and server deployment and synchronization. Also require to maintain white list and blacklist of sites. Real time implementation considerations
Email spoofing detection based [5]	Authors proposed a novel key distribution architecture and identity based digital signature for making email trustworthy and hence detecting & mitigating spam mails by detecting email spoofing	**Fighting phishing attacks lightweight trust architecture for detecting phished mails.** B. Adida et.al 2005	Upgraded email client and at least one key server.	The scheme is lightweight neither pre-established public key infrastructure nor cooperation between email domains is required. all legitimate uses of email remain fully functional after the changes required by the scheme	Real time implementation considerations. Requires noticeable changes in the email service provider's side
Picture passwords Based [6]	Author has shown the usability of Picture passwords and shown how picture keypads can be used for entering credentials instead of typing through keyboard. A number of features of keypad are personalized to the user such as background color border design of keypad which differ from other users, and selected from the user's stored account record by means of the user's username. This provides protection against phishing, by alerting the user when any changes to their familiar keypad 'look-and-feel' occur, which is unknown to the phisher.	**The usability of picture passwords** N. Fraser	Set of pictures from which a subset of pictures will be issued as password to a particular user	Avoid logging by key loggers, also it is impossible for a user to disclose their password on a randomly generated phisher keypad as it is hard for a phisher to randomly generate a keypad that contains all picture necessary for entering the password by a user.	It will be complex from user's perspective to enter the password time during login by picture keypad and will require user training.
Dynamic security skin based [7]	Authors proposed two interaction techniques to prevent spoofing. 1. Browser extension provides a trusted Window in the browser for username and password entry. A photographic image for creating a trusted path between the user and the window so as to prevent spoofing of the Window and text entry fields. 2. The scheme allows the remote server to generate a Unique abstract image for individual user for each transaction. The image will create a "skin" that will automatically customize the Window or the user interface elements in the content of a remote web page. The extension will allow the browser to inde-	**The Battle Against Phishing: Dynamic Security Skins** R. Dhamija, J.D. Tygar 2005	Configured remote server and browser extension.	To authenticate, the user has to recognize only one image and remember one low entropy password, no matter how many Servers he wishes to interact with. To authenticate content from an authenticated server, the user only needs to perform one visual matching operation to compare two images.	Increases the complexity of user interface, require initial user training requires client server interaction each time a transaction is performed. Extended browser window, increases the complexity of user interaction.

	pendently compute the image it expects to receive from the remote server. To authenticate content from the server, the user can visually verify that the images match.				
Browser Extension Based [8]	Authors described a browser extension, PwdHash that transparently produces a different password for each site, which improves web password security and defends against phishing and other attacks. Browser extension apply 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 which is stored on the client machine.	**Stronger Password Authentication Using Browser Extensions** B. Ross et.al 2005	Browser Extension, a good cryptographic hash function.	The scheme requires no changes on the server side. Theft of password received at one of the website will not reveal the password that will be used at another website.	Implementing this password method securely and transparently in a web browser extension turns out to be quite difficult
Smart card based [9]	Authors proposed two solutions: 1. Short-time password solution. This authentication scheme uses an offline card reader and a smart card to produce short-lived passwords on demand. 2. Certificate-based solution. This authentication scheme uses a secure online card reader, the FINREAD card reader, and a smart card to sign SSL/TLS challenges on demand	**Secure Internet Banking Authentication,** A. Hiltgen, et.al 2006	Java Applet Websites that can detect FINREAD card reader, Card Readers.	The user's credentials are stored on the smart card and can only be accessed via an offline smartcard reader, so malicious software can't get the user's symmetric cryptographic key or related functionality. Scheme effectively thwarts both offline credential-stealing attacks as well as online channel-breaking attacks.	Necessity of mobile equipment's. Require major changes in underlying system. Complex.
QR Code based [10]	Author proposed an anti-phishing single sign-on (SSO) authentication model using QR code. This scheme is secure against phishing attack and even on the distrusted computer environment. Scheme consists of three phases: login request phase, QR code generation phase, and verification phase.	**A mobile based anti-phishing authentication scheme using QR code**, K. Choi et.al 2011	QR (Quick Response) Code reader, extended authentication server, External Mobile device.	User can access the web sites in online Environment of distrust local computer and web server using mobile device. Even if the user's sensitive information is exposed, attacker cannot obtain the mobile information because user data is encrypted by the mobile device. Users can check the web server whether this server is the phishing server through the extended authentication server	Complex Scheme for deployment Requires an extended authentication server, whose reliability is a concern. Requires a secure external mobile device. Feasible, efficient and transparent deployment in real world is a question.

10. Extended authentication schemes for prevention of Phishing requires configuration, management and security consideration for extended authentication servers which are used to authenticate the web-servers a user is communicating with. Also it increases the communication time and cost for each user login.

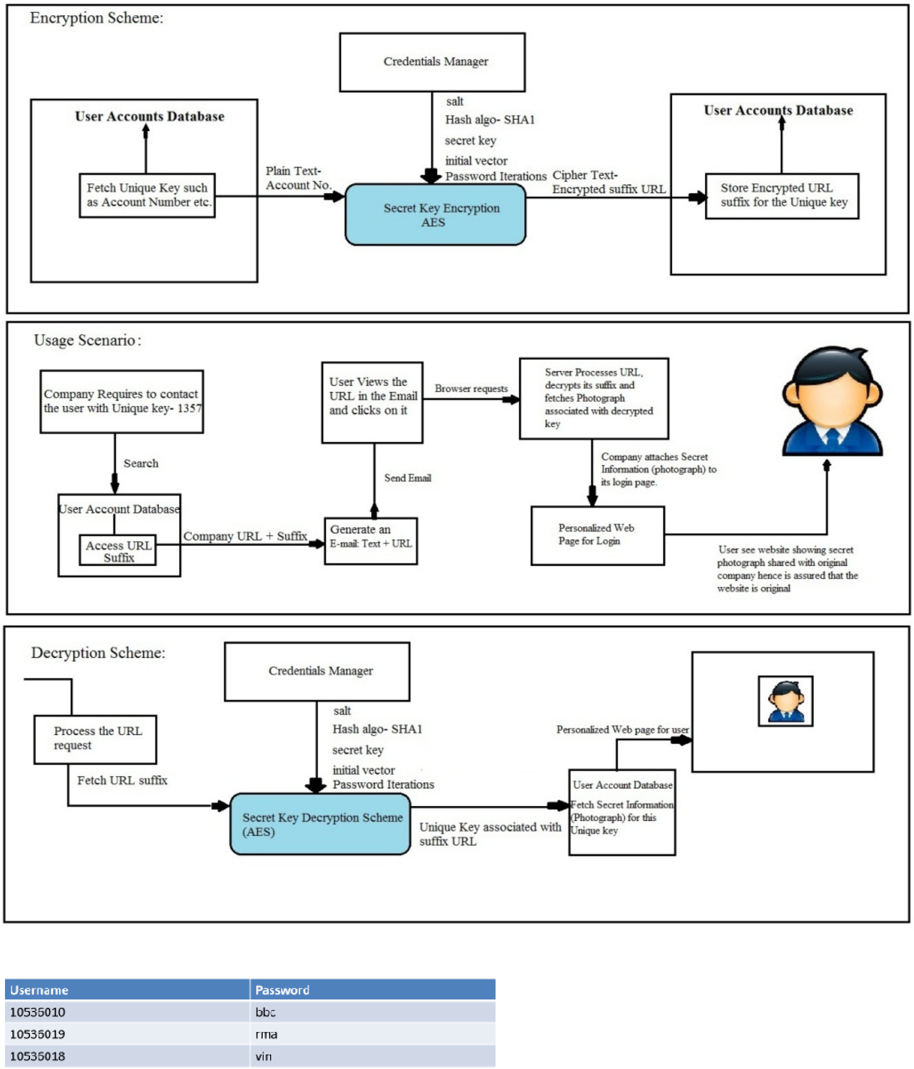
3 Personal Secret Information Based Authentication towards Preventing Phishing Attacks

Our proposed sheme is for prevention of phishing attacks by providing users a way to verify the originality of the website they are logging with while they click on a link in the e-mail that comes to their E-mailbox. This is achieved by using a piece of secret information that can be a photograph or a key which is shared between the user and the website and is provided by the user at the time of online account creation. In our implementation we will use a photograph as a piece of secret information. The overall architecture proposed is shown in fig1.

The architecture proposed require minimal changes to the underlying database that is used by websites for storing user credentials. Generally websites of online banking, social networking and others store userid and passwords as secret credential for a unique user and the verification includes checking these credentials when a user login with them. Our proposed scheme requires that websites should include some more user secret information to prevent phishing and use them in a way that will help the user to discriminate between original and phished websites. By secret information we mean userid, password as usual with the additional use of a user's photograph or a secret phrase.

The overall scenario and the underlying scheme we propose is based on the assumption that if a user can see the login pages of their websites personlaized then there will be low chances that they will fall for phishing as a phisher cannot provide such a personalization on a phished website as he is unaware of the secret information shared between user and the original company website and which is being used as a way to provide personalized experience to each unique user.

The personalization for each user while they click on the links sent to them through email from original companies is achieved by storing URL suffix for each user which is encrypted userid and will be used with the compaanies URL whenever company wants any communication. This will result in URL suffixes for each individual user which are stored with the user credentials in the database. these will be then sent to the user whenever company wants to contact the specific customer. when the user click on such a link the url suffix will be retrieved and processed to get the user id associated from where he can extract the secretv information shared with the website and display them at appropriate places during login to provide user a kind of personlization. The Encryption scheme for converting unique user information such as user id's to URL suffixes with the decryption scheme showing the server side processing of URL to obtain the userid for providing user personlization is shown in Fig.1 also explains the usage scenario in which the scheme will be deployed and used.


Encryption Scheme:
Credentials Manager
User Accounts Database
Fetch Unique Key such as Account Number etc.
Plain Text- Account No.
salt
Hash algo- SHA1
secret key
initial vector
Password Iterations
Secret Key Encryption AES
Cipher Text- Encrypted suffix URL
User Accounts Database
Store Encrypted URL suffix for the Unique key
Usage Scenario:
Company Requires to contact the user with Unique key- 1357
Search
User Account Database
Access URL Suffix
Company URL + Suffix
Generate an E-mail: Text + URL
Send Email
User Views the URL in the Email and clicks on it
Browser requests
Server Processes URL, decrypts its suffix and fetches Photograph associated with decrypted key
Company attaches Secret Information (photograph) to its login page.
Personalized Web Page for Login
User see website showing secret photograph shared with original company hence is assured that the website is original
Decryption Scheme:
Credentials Manager
Process the URL request
Fetch URL suffix
salt
Hash algo- SHA1
secret key
initial vector
Password Iterations
Secret Key Decryption Scheme (AES)
Unique Key associated with suffix URL
User Account Database
Fetch Secret Information (Photograph) for this Unique key
Personalized Web page for user

Username	Password
10535010	bbc
10535019	rma
10535018	vin

Fig. 1. Proposed Architecture

3.1 Encryption Scheme

When a user supplies the user credentials in the form of userid, password and secret information(photograph) the information will be stored as usual in the companies database. From there the userid (unique key) is extracted and is encrypted by a symmetric encryption scheme (AES) to develop a URL suffix that will be stored in the user database with that user id and is then sent as URL suffix with the companies URL link that company will sent to the user for logging in emails.

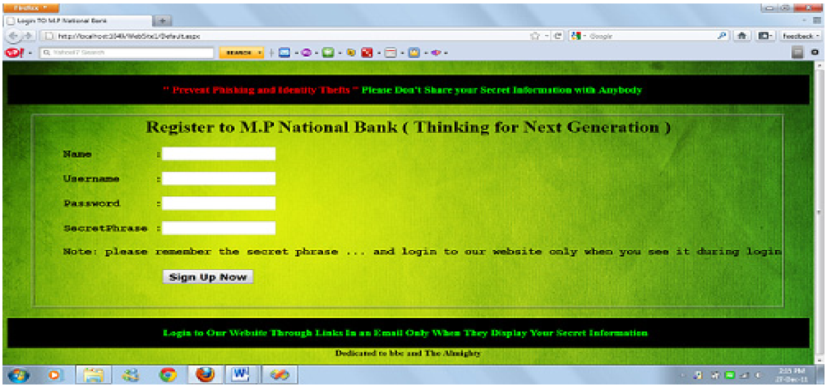
3.2 Decryption Scheme

Whenever a user will click on the link in the mail from the original companies website the link is processed at the server side. The processing includes fetching the URL suffix associated with the URL and then decrypting it with the symmetric decryption scheme(AES) to obatin the userid which was encrypted. the user id is then used to extract the secret information which is photograph associated with the user and then eventually displaying it on the login window. This will make sure the user that the page with which is he logging with is original as phisher has no knowledge of the secret photograph he shared with the company during account creation.

Both Encryption and decryption schemes require the usage of a trusted component at the server side that will store the secrets for encryption and decryption scheme. we call it in our scheme as Credentials manager. for encryption and decryption we have proposed Advanced Encryption standard (AES). The initial study shows that AES is a good symmetric enryption scheme as the only way of breaking it is through brute force attacks and those kind of attacks on hug key sizes as provided by AES are proven to be difficult and is also used in [10]. The credential manager will store the information for the AES encryption scheme and are as follows:

1. Salt which act as second secret password
2. Hash Algorithm can be SHA-1 or MD-5.
3. Secret key used for encryption and decryption
4. Initial vector which is an collection of 16 ASCII characters
5. Password iteration that defines the no of times the algorithm is run on the plain text.

The screenshots of our prototype implementation are shown below:



" Prevent Phishing and Identity Thefts " Please Don't Share your Secret Information with Anybody

Register to M.P National Bank (Thinking for Next Generation)

Name :

Username :

Password :

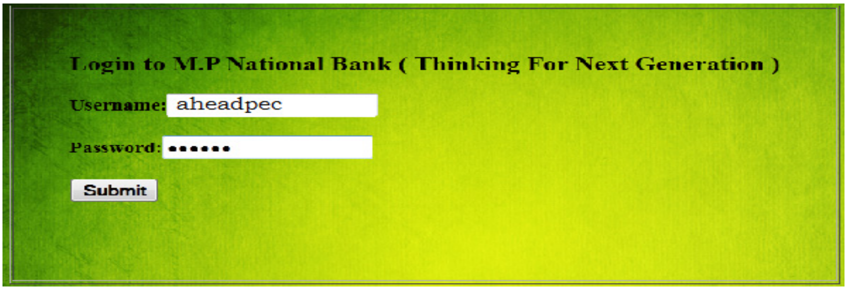
SecretPhrase :

Note: please remember the secret phrase ... and login to our website only when you see it during login

Login to Our Website Through Links In an Email Only When They Display Your Secret Information

Dedicated to bbc and The Almighty

Fig. 2. Sign up page of a website as per proposed scheme

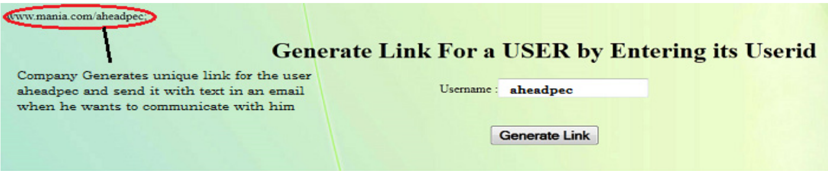


Login to M.P National Bank (Thinking For Next Generation)

Username: aheadpec

Password: ●●●●●●

Fig. 3. Login page



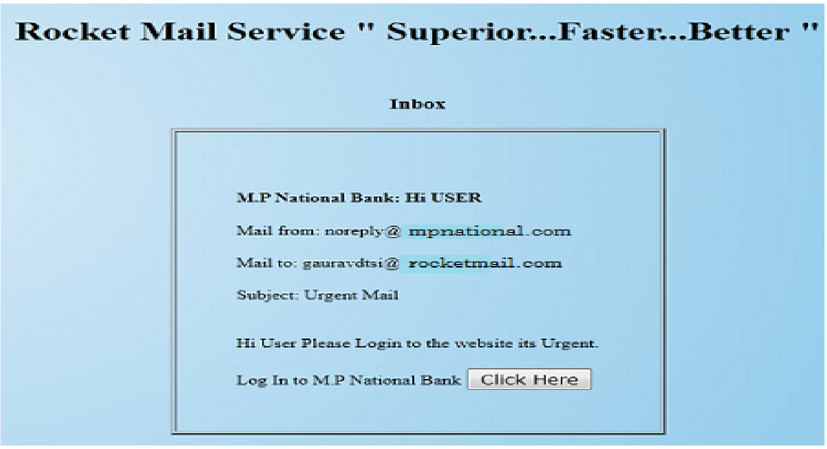
www.mania.com/aheadpec;

Company Generates unique link for the user aheadpec and send it with text in an email when he wants to communicate with him

Generate Link For a USER by Entering its Userid

Username : aheadpec

Fig. 4. Comapny Generating URL for user aheadpec



Rocket Mail Service " Superior...Faster...Better "

Inbox

M.P National Bank: Hi USER

Mail from: noreply@ mpnational.com

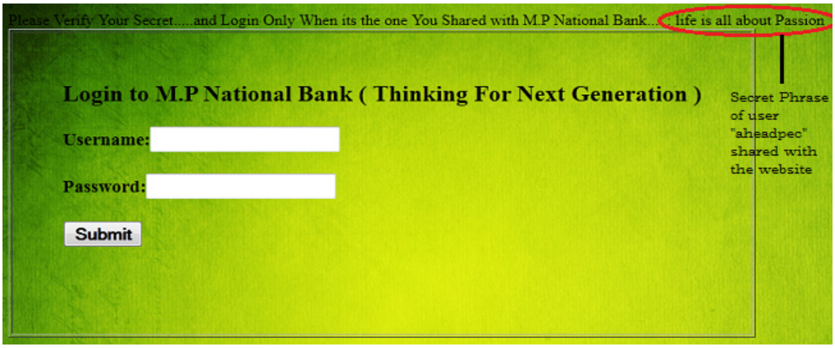
Mail to: gauravdtsi@ rocketmail.com

Subject: Urgent Mail

Hi User Please Login to the website its Urgent.

Log In to M.P National Bank

Fig. 5. Mail Sent from company to user aheadpec



Please Verify Your Secret.....and Login Only When its the one You Shared with M.P National Bank... : life is all about Passion

Login to M.P National Bank (Thinking For Next Generation)

Secret Phrase of user "aheadpec" shared with the website

Fig. 6. Login page showing secret phrase aheadpec shared with website during sign up

4 Advantages of Proposed Scheme

The advantages of our scheme wll provide compared to other techniques are as follows:

1. Our Proposed scheme does not require any kind of support from spam and phished mail filters provided by email service providers and also don't rely on their accuracy in detecting phished email.
2. This scheme can be implemented in real time by companies with minimal changes to their server side processing.
3. Key management is not a task as no sharing of key is done anywhere in the scheme. However the credentials managers have to be designed in a way so that the credentials can be protected from attackers reach. Also credentials manager can refresh the scheme by changing the values of the credentials stored after a certain period of time.
4. The scheme can rely on a single unique key used for encryption and decryption of all user ids. But generally credentials manager can implement numerous other schemes in which he can allot certain group of user id's a different set of credentials for encryption and decryption and the other group a different one that will eventually increase the security.
5. Our scheme require no changes in the browser or the at the client machine.
6. There is no requirement for any external authenticating device.
7. It requires no user training and is not annoying compared to other techniques. Also user doesn't have to remember the position, color, shape and sizes of any browser window or watermark Image.
8. Our Scheme doesn't require any special external card readers or tokens as used in some techniques for phishing preventions and hence our solution doesn't add cost and complexity to the underlying system.
9. There is no requirement for extended authentication server which cuts off extra server maintenance and configuration with reduced time per login.

5 Conclusion and Future Work

We have proposed a novel scheme based on personal secret information for authentication towards preventing Phishing attacks which are launched through Phished website links in emails. The Scheme is easy to deploy in real world scenario with minimal changes and better efficiency. A working prototype of the proposed scheme is developed and its accessment on various measures such as communication cost, time and efficiency is under study.

In future we will try to apply this technique in a way to prevent Web Phishing which occurs when a user reaches a Phished website through typing mistakes on browsers etc. and not from links in Phished emails.

References

1. Singh., A.P., et al.: Detection and Prevention of Phishing Attack Using Dynamic Watermarking. Information Technology and Mobile Communication Communications in Computer and Information Science, Part 1 147, 132–137 (2011), doi:10.1007/978-3-642-20573-6_212011
2. Liou, J., et al.: A Sophisticated RFID Application on Multi-Factor Authentication. In: 2011 Eighth International Conference Information Technology: New Generations (ITNG), Las Vegas, pp. 180–185 (2011), doi:10.1109/ITNG.2011.38
3. Parno, B., Kuo, C., Perrig, A.: Phoolproof Phishing Prevention. In: Di Crescenzo, G., Rubin, A. (eds.) FC 2006. LNCS, vol. 4107, pp. 1–19. Springer, Heidelberg (2006)
4. Florencio, D., Herley, C.: Password Rescue: A New Approach to Phishing Prevention. In: Proceedings of the 1st USENIX Workshop on Hot Topics in Security, HOTSEC (2006)
5. Adida., B., et al.: Fighting Phishing Attacks: A Lightweight Trust Architecture for Detecting Spoofed Emails. In: DIMACS Workshop on Theft in E-Commerce (2005)
6. Fraser, N.: The usability of picture password (unpublished)
7. Dhamija, R., Tygar, J.D.: The Battle Against Phishing: Dynamic Security Skins. In: Proceedings of the 2005 symposium on Usable privacy and security, SOUPS (2005)
8. Ross, B., et al.: Stronger Password Authentication Using Browser Extensions. In: Security 2005 Technical Program (2005)
9. Hiltgen, A., et al.: Secure Internet banking authentication. IEEE Security & Privacy 4(2), 21–29 (2006), doi:10.1109/MSP.2006.50
10. Kyeongwon, C., et al.: A mobile based anti-phishing authentication scheme using QR code. In: 2011 International Conference on Mobile IT Convergence (ICMIC), September 26-28, pp. 109–113 (2011)
11. APWG.: Origins of the Word "Phishing", `http://www.antiphishing.org/word_phish.html`