International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 4, April 2013 **ISSN 2319 - 4847**

Crossbreed Advanced Security against Pishing and Spoofing

Deepinderjeet Kaur Dhaliwal[1], Amandeep Kaur[2]

Research fellow[1], Assistant Professor[2],
Department of Computer Science and Engineering,
Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, INDIA

ABSTRACT

Phishing /Pharming/ Web Spoofing (Felten et al. 1997, Geer 2005, Anti-Phishing Working Group 2005) attacks are widely used to gather user personal information, including usernames and passwords. One possible scenario for such an attack arises when an attacker creates a spoofed web site that looks identical to a genuine web site, and convinces the victim to visit the spoofed web site e.g. by including a URL in a faked email. The phishing attacks can also be used to protect against other online attacks. The act of sending an e-mail to a client fallaciously declares to be a recognized genuine organization in an Endeavour to deceive the client into compromise confidential information that will be used for identity theft. In the first section of the paper analyze the Phishing Definition and Phishing Techniques. In the second section of the paper described the related work. In the third section is analyzing the Properties of Phishing. In the fourth section described different steps of a typical Phishing. In the fifth section described effectiveness of SSL in the indicators of HTTPS and in the sixth section analyze the demonstration of anti phishing scheme. Finally present the Conclusion & future works with the references.

Keywords- Email Phishing, URL, Domain spoofing, SSL/TLS protocol, Phisher and Phishing Message.

1. INTRODUCTION

Phishing is a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' condential or sensitive credentials by mimicking electronic communications from a trustworthy or Public organization in an automated fashion Email[1]. Phishing in which someone tries to trick you into revealing information by sending fake emails that look legitimate and remains one of the biggest online threats. One of the most methods that scammers employ is something called domain spoofing [2]. In this technique someone sends a message that seems legitimate when you look at the "From" line even though it's actually a fake. Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information. Phishing is a form of online identity theft associated with both social engineering and technical subterfuge [3]. Attackers might send millions of fraudulent e-mail messages that appear to come from Web sites you trust, like your bank or credit card Company, and request that you provide personal information In a phishing attack, the phisher duplicates the original website and promotes the client to provide the personal information, for doing so phisher generally uses the email in which some hyperlinks are shown as original web link or web address, but these hyperlinks contains the address of duplicate or mimic website which is made by Phisher when client receive the email from spoofed domain, they believes this mail is generated from original domain and reply these email[4]. SSL/TLS that is of particular interest here is the Certificate Request protocol message, which can be used to request a client-side web browser to provide a public key certificate for authentication of the client to the server. If sent by the web server, the web browser replies by sending a copy of the client certificate selected by the user, and a proof of knowledge of the associated private key, i.e. by signing the 'Certificate Verify' SSL handshake message. However, this element of the protocol is typically not used, since most users do not have personal public key certificates. Phishing and Web spoofing have proliferated and become a major nuisance on the Internet. Attempts to stop phishing by preventing a user from interacting with a malicious web site have shown to be ineffective. The SSL/TLS protocol provides data integrity and data confidentiality via the 'record protocol' and entity authentication by means of the 'handshake protocol'.

2. RELATED WORK

2.1 Mitesh Bargadiya[5] described an analysis of the phishing and the Line of attack in which it affect the client & association. This paper present an analysis of most frequently used system of phishing and reviews some anti –Phishing approaches. The act of sending an e-mail to a client fallaciously declares to be a recognized genuine organization in an endeavour to deceive the client into compromise confidential information that will be used for identity theft. The e-mail

endorse the client to visit a mimic Web site where they are request to update individual information, such as credit card number, bank account numbers, date of birth, confidential passwords etc., the above process is known as Phishing. This paper approached, "anti-Phishing Design uses Mutual Authentication Approach" With mutual authentication, a connection can occur only when the client trusts the server and the server trusts the client. The process of this paper can be efficiently reducing the risk of phishing in very simple steps to naïve computer user.

2.2 Vijaykumar kangala[6] is described that the phishing WebPages strategy based on optical semblance assessment. An approach to phishing webpage strategy based on optical semblance assessment is proposed, which can be utilized as a part of an enterprise solution to anti-phishing. The approach first decomposes the web pages into salient block regions. The optical semblance between two web pages is then evaluated in three metrics: block level similarity, layout similarity, and overall style similarity. A webpage is reported as a phishing suspect if any of them is higher than its corresponding preset threshold. Preliminary experiments show that the approach can successfully detect those phishing web pages with few false alarms at a speed adequate for online application.

2.3 Jakobsson M. Modeling[7] is described Phishing is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party. It should detect online crime by that the phisher could then notify the victim of a "security threat." The context aware phishing an attacker would gain the trust of victims by obtaining information about their bidding history or shopping preferences their banking institutions or their mothers' maiden names.

2.4 Ronnie Manning[8] is described that the Phishing is an attempt to commit fraud via social engineering. The impact is the breach of information security through the compromise of confidential data. Customers can access their banking accounts from anywhere in the world using their login ID and password. However, the use of password does not provide adequate protection against Internet fraud such as phishing. Phishing exploits this vulnerability to fraudulently acquire sensitive personal information, such as username, passwords and/or credit card details.

2.5 Hardik Desai[9] is described that Phishing is an attempt to commit fraud via social engineering. The impact is the breach of information security through the compromise of confidential data. Customers can access their banking accounts from anywhere in the world using their login ID and password. However, the use of password does not provide adequate protection against Internet fraud such as phishing. Phishing exploits this vulnerability to fraudulently acquire sensitive personal information, such as username, passwords and/or credit card details. Usually this is achieved by masquerading as a trustworthy person or business with an apparently legitimate request for information. In this paper we have proposed a new approach named as IAPC.

2.6 Juan Chen and Chuanxiong Guo[10] is described that Phishing has becoming a serious network security problem, causing finical lose of billions of dollars to both consumers and e-commerce companies. And perhaps more fundamentally, phishing has made e-commerce distrusted and less attractive to normal consumers. This paper studied the characteristics of the hyperlinks that were embedded in phishing e-mails. We then designed an anti-phishing algorithm, Link- Guard, based on the derived characteristics. Since Phishig- Guard is characteristic based, it can not only detect known attacks, but also is effective to the unknown ones.

2.7 Yue Zhang, Serge Egelman, Lorrie Cranor and Jason Hong[11] is described that the anti-phishing tools that were examined in this study left a lot to be desired. Spoof Guard did a very good job at identifying fraudulent sites, but it also incorrectly identified a large fraction of legitimate sites as fraudulent. The performance of the other tools varied considerably depending on the source of the phishing URLs. Of these other tools, only IE7 was able to correctly identify over 60% of phishing URLs from both sources, but it still missed 25% of the APWG phishing URLs and 32% of the phishtank.com phishing URLs. The only tool we tested that is known to make no use of blacklists was Spoof Guard. While it was able to identify the majority of phishing sites using only heuristics, it still missed some phishing sites and it had a very high false positive rate.

2.8 Engin Kirda, Christopher Kruegel [12] is described that Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. This paper presents a novel browser extension; AntiPhish aims to protect users against spoofed web site-based phishing attacks. To this end, AntiPhish tracks the sensitive information of a user and generates warnings whenever the user attempts to give away this information to a web site that is considered untrusted.

2.9 Rachna Dhamija, J. D. Tygar and Marti Hearst[13] is described that Why Phishing Works that this study illustrates that even in the best case scenario, when users expect spoofs to be present and are motivated to discover them, many users cannot distinguish a legitimate website from a spoofed website.

2.10 Mallikka Rajalingam, Saleh Ali Alomari, Putra Sumari[14] is described that the combination of phishing of the social engineering which provide personal information, usually for the monetary gain of the attacker or Phisher. In this it present an effective image-based anti-phishing scheme based on discriminative key point features in WebPages. It uses an invariant content descriptor, the Contrast Context Histogram (CCH), to compute the similarity degree between suspicious pages and authentic pages.

2.11 Adil Alsaid and Chris J. Mitchell[15] is described for secure web sites which uses the SSL/TLS protocol for server authentication. Mutual authentication support is provided by SSL/TLS which uses both server and client authentication. This feature of SSL/TLS is not used by most web sites because not every client has a certified public key. Instead user authentication is typically achieved by sending a password to the server after the establishment of an SSL-protected channel. Certain attacks rely on this fact, such as web spoofing and phishing attacks. This paper described the issue of online user authentication is discussed and a method for online user authentication using trusted computing platforms is proposed.

2.12 Peter Finn Markus Jakobsson [16] is described that standards and procedural aspects of setting up and conducting phishing experiments which drawing on experience gained from being involved in the design and execution of a sequence of phishing experiments. This paper described the roles of consent, deception, debriefing, risks and privacy and how related issues place IRBs in a new situation.

3. PHISHING TECHNIQUES

A. Phishing: - Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. The most common way of hacking them is phishing. The common type of phishing is Fake Login Page. The victim is anyhow anyway made to enter his credentials in fake login page which resembles the genuine login page and gets hacked.

B. Spear Phishing: - Spear phishing targets at a specific group. So instead of casting out thousands of emails randomly, spear phishes target selected groups of people with something in common, for example people from the same organization [17].Spear phishing is also being used against high-level targets, in a type of attack called whaling. Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success.

C. Clone Phishing: -A type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address taken and used to create an almost identical or cloned email. The attachment or Link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a re-send of the original or an updated version to the original. This technique could be used to pivot from a previously infected machine and gain a foothold on another machine, by exploiting the social trust associated with the inferred connection due to both parties receiving the original email [18].

D. Phone Phishing:- This type of phishing refers to messages that claim to be from a bank asking users to dial a phone number regarding problems with their bank accounts. Traditional phone equipment has dedicated lines, so Voice over IP, being easy to manipulate, becomes a good choice for the phisher. Once the phone number, owned by the phisher and provided by a VoIP service is dialled that voice prompts tell the caller to enter her account numbers and PIN. Caller ID spoofing, which is not prohibited by law, can be used along with this so that the call appears to be from a trusted source [19].

4. PROPERTIES OF PHISHING

Many research methods are proposed to overcome the phishing or spoofing but they are not stop phishing completely, we are discussing some property of the previously proposed system:

A. Use of Logo & Icon property: - We must go to unexpected extent to avoid people from automatically conveying trust based on logos unaccompanied [20]. This principle applies to the design of security sign and icons as well. For example, client often implicitly place trust in security icons SSL lock icon, whether they are legitimate or not.

B. Authentication Protocol: - Client-server authentication is done by many secure authentication protocol and algorithms, designer use only such kind of authentication protocol and algorithms which are easily available, easy to implement, cost effective and required minimum communication bandwidth between client & server. Now hashes are used to decrease the amount of data that needs to be transmitted. The hash function are cryptographically strong, e.g. RIPEMD-160, MD5 and SHA[21].

C. Certificate Authority: - Certificate authorities concern digital certificates that enclose a public key and the identity of the proprietor. When a user attempt to access an unidentified URL, the web browser will contact the certificate authorities to authenticate the public key of the URL. The corresponding private key is not also made accessible publicly, but kept secret by the end user who generated the key pair. The certificates also an authentication by the certificate authorities that the public key limited in the certificate belongs to the person proprietor entity noted in the certificate [22].

D. Browser Vulnerabilities:

Old version of the browsers are not able to check the phishing site but now many browser come with add-ons & toolbars, which are available to prevent phishing but they are not much effective.

E. The user psychology:- General behaviour of user to any security message or warning is “they are interrupting “and user continue to accomplished the task and ignoring the security message partially or completely too much security

become bottle neck, but few user may check the padlock icon, certificate & certificate authority as well as domain. Ignoring the security message, this kind of user psychology helps the phisher but give more burdens to the security designer.

5. STEPS OF A TYPICAL PHISHING

- A phishing message is sent to a list of targeted emails.
- The message's title is written to capture users' attention so it usually includes words like alert, update, action required, important notice etc.
- The sender's address is filled with a forged email belonging to the service provider it claims to come from or with a similar address when the target is required to reply to the email.
- The message body directs users to send their information using an attached form requesting personal information or via a link to a clone of the system.
- The links included in the message are posted as clickable images or HTML hyperlinks to hide the real address from theuser(e.g.<ahref='http://58.30.143.198/mobile/online.hsbc.co.uk/'> http://online.hsbc.co.uk/).
- The message style imitates the design of the original service provider and includes logos and email signatures to cause visual deception to users, hence giving them a false sense of security. Since the message is sent to a large number of users, it is usually impersonalized and includes generic greetings. However, some of the recent phishing scam greeted users by their names or email addresses.
- A large portion of the reviewed phishing messages included spelling mistakes in the title or body of the emails.
- The phishing site is a partial clone of the system. Attackers copy the exact HTML tags of useful pages e.g. the user authentication pages to capture sensitive information, but not everything. Instead, they include links to the original system if the user tries to navigate.
- His domain name of the targeted service is used as part of the spoof address to trick people, mostly as a sub domain e.g. http://paypal.com.pltx.info/.
- After logging the victim's response, a typical phishing site generates a feedback and forward to the original system.
- Frames and pop-ups are used at times to place a spoof form on a legitimate website instead of designing a clone of the system. However, this technique is less popular.

6. EFFECTIVENESS OF SSL IN THE INDICATORS OF HTTPS

In the current scenario, there are several sites which are not secure as per the HTTPS security rule and SSL certification but the browser hardly recognizes these parameters for processing. Our basic problem is to create a browsing system which would consist a log files for the SSL certification and HPPS content problem. When the user would surf through the browser, it would check the contrast from the log file and will confirm it whether it is secured in terms of HTTPS and further on the same procedure would be followed for SSL certification error. A warning message will be issued if we get a negative feedback from the browser log file and the user will be warned for the same. By this manner we can increase the security for the browsing system and from the unauthorized access of the content which are phishing. The effectiveness of phishing bother is reducing when users can consistently differentiate and authenticate security sign. Sorry to say, current and related application programs have complex design, then clients have the subsequent problems:

A. Source Identification: - Phishing attack starts with various URL techniques such misleadingly named link, cloaked links, Redirected links, Obfuscated links, programmatically obscured links and Map links [23]. Client cannot correctly determine the domain name of the website page with URL https://www.icicionline.com/dsw?psw/index12365was considered significantly less trustworthy than a page whose URL was http://www.icici.com. Here, the material of these two pages was the same, and the first page was actually SSL confined, but was silent given an inferior rating [24].

B. The Client Knowledge & Locality: - When client receive the misguiding email for phishing site which may be look same as original email, educated or technically sound user can primary check this mail is authentic or not by observing the content & Language of the email but uneducated user believes this mail is from genuine website and may provide desire personal information to the phisher [25]. Locality can also give some contribution in decision making we can assume that urban user may aware form this kind of scam and take more precaution with compare to rural user.

C. Misguided Email: - Various phishing emails were present notice on spelling without help. Clients not often illustrate to notice the presence of a disgusting grammatical mistake. Many Clients were doubtful of emails that were not mark by an individual but in its place by a designation only. Similarly, Clients disapprove of email messages that initiate them not to respond. Some genuine sources were particular a low rating due to "unprofessional design". Clients disagree that phishers do not need legal disclaimers, and do not care about authorized disclaimers. Therefore, phishers are not expected to include such sentences in messages [26]. D. hyperlinks Phisher generally sends an email to misguide the user and promote to click on the give hyperlink in order to access own account immediately, when user click the hyperlink, user is redirect to fake website and phisher get ID as well as Password.

7. DEMONSTRATION OF ANTI- PHISHING SCHEME

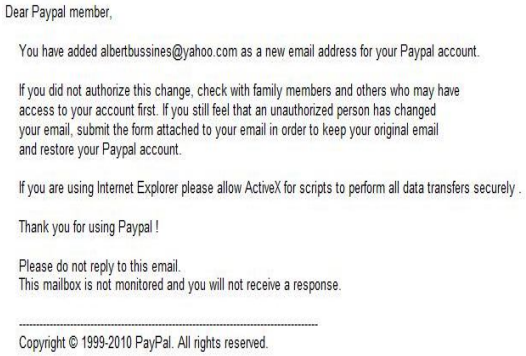
The demonstration of the anti-phishing schemes presented in fig 1 clearly addresses the human factor as the weakest part in the resisting procedure. Even when the technical solution successfully defines a webpage as a definite spoof, reports suggest that security alerts are dismissed or ignored by the vast majority of users (Miller, 2005) (Dhamija et al., 2006) (Wu et al., 2006) (Downs et al., 2006). Reasons resolved from the examples discussed earlier dissect the human factor into the following elements:

1) Knowledge: users are not security specialists. Many of them are not acquainted with technical details and do not understand how the service or the anti-phishing scheme works. Figure 1 illustrated an example of a phishing attempt designed to exploit users vulnerable to this attack due to their lack of knowledge. Hence, sensitive details can be obtained through second channels such as online forms and emails.

2) Alertness: even if users are trained on a security scheme, they are not conscious at all times to respond respectively to security warnings. Security indicators might not be recognized. For example, the absence of the server image in the Pass Mark experiment (Stone, 2007) was not noticed as discussed earlier.

3) Motivation: users are not self-motivated to continuously examine security. For example, while the legitimacy of a site seal can be verified via a third-party website, a spoofed seal could pass unchecked since it is inconvenient for users to examine it every time they use the service. Another example was the Pet name tool; to work, it requires end users to manually customize e-commerce sites with identifiers, memorize the names given and recognize them in the future. Only highly motivated users might customize all websites.

4) Concern: lack of concern about warning messages. False-positive warnings can be a reason for that as genuine pages can be erroneously highlighted as a spoof by some security tools or correctly highlighted with other types of warning message. It is observed that when more alerts are generated, users start ignoring them at a higher rate.



Dear Paypal member,

You have added albertbussines@yahoo.com as a new email address for your Paypal account.

If you did not authorize this change, check with family members and others who may have access to your account first. If you still feel that an unauthorized person has changed your email, submit the form attached to your email in order to keep your original email and restore your Paypal account.

If you are using Internet Explorer please allow ActiveX for scripts to perform all data transfers securely .

Thank you for using Paypal !

Please do not reply to this email.
This mailbox is not monitored and you will not receive a response.

Copyright © 1999-2010 PayPal. All rights reserved.

Figure 1: Sample of a phishing message targeting PayPal users.

HSBC
The world's local bank

Dear HSBC Bank UK Cardholder,

You have one new message. you are requested to

Log on to your account to view message.

Thanks for your co-operation. Fraud Prevention Unit Legal Advisor HSBC Bank UK.
Please do not reply to this message. For any inquiries, contact Customer Service.
© 2010 HSBC Bank UK. National Association, Inc.

Figure 2: Sample of a phishing message targeting HSBC users.

8. CONCLUSION & FUTURE WORK

Phishing is a web authentication problem hence two schemes were developed as a factual proof that a better design of the authentication system can resist more phishing attempts and provide better protection. Phishing resistance is hard due to a number of factors, essentially the human factor accompanied by the sophistication of recent attacks. In the current scenario, there are several sites which are not secure as per the HTTPS security rule and SSL certification but the browser hardly recognizes these parameters for processing. Our basic problem is to create a browsing system which would consist a log files for the SSL certification and HPPS content problem. When the user would surf through the browser, it would check the contrast from the log file and will confirm it whether it is secured in terms of HTTPS and further on the same procedure would be followed for SSL certification error. By this manner we can increase the

security for the browsing system and from the unauthorized access of the content which are pishing .In the work till now we have developed a browsing system which can restrict the URL which has been entered by the administrator to secure the browser from spoofing. Security groups and online service providers must develop methods to educate users about the recent tricks used by phishers. A good example is a game called 'Phish/No Phish' developed by VeriSign (hosted at https://www.phish-no-phish.com) for users to experiment their ability to spot. In this paper we perform an analysis of the phishing techniques and properties and the step of the typical phishing. We also present an analysis of most frequently used system of phishing and review some anti –Phishing approaches. In our proposed scheme, general user easily communicates to Web Server with higher extent of security & handles the phishing attack. In the future an automated system can be created so that if the contents of the website are finding phished they can be removed automatically by the creation of phishing automated tool and we can use stronger Encryption & Decryption Algorithms, Hash Function algorithms to improve the overall security of communication.

REFERENCES

[1] Markus Jakobsson and Steven Myers. Phishing and countermeasures: understanding the in- creasing problem of electronic identity theft. John Wiley & Sons, Inc., 2007.

[2] Wikipedia. Phishing | Wikipedia, the free encyclopedia. http://en.wikipedia.org/w/index.php?title=Phishing&oldid=484977983, 2012.

[3] Anti Phishing Working Group. Origins of the word \phishing". http://www.antiphishing. Org/word_phish.html.

[4] Mark Hughes (4 January 2008). "Logos that became legends: Icons from The independent, http://www.independent.co.uk./news/media/logos-that became-legends-icons-from-the-world-of advertising-768077.html. Retrieved 2008-04-27.

[5]Mitesh Bargadiya et al. / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (3), 2010, 175-178

[6] Vijaykumar kangala et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2

[7] Jakobsson M. Modeling and Preventing Phishing Attacks,
Phishing Panel of Financial Cryptography, 2005.

[8] Ronnie Manning, "Phishing Activity Trends Report", AWPG, January-June, 2011.

[9] "Hardik Desai" et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1), 2013, 34 – 38

[10] "Juan Chen and Chuanxiong Guo""Online Detection and Prevention of Phishing Attacks (Invited Paper)" Vol. 5 IJCSS 2009".

[11] "Yue Zhang, Serge Egelman, Lorrie Cranor, and Jason Hong" "Phinding Phish: Evaluating Anti-Phishing Tools"" Vol 4 IJCSS 2011".

[12] "Engin Kirda, Christopher Kruegel" Protecting Users Against Phishing" The Computer Journal Vol. 00 No. 0, 2005".

[13]"Rachna Dhamija, J. D. Tygar and Marti Hearst" "Why Phishing Works""Human Factors in Computing Systems, April 2006"

[14] "Mallikka Rajalingam, Saleh Ali Alomari & Putra Sumari" "Prevention of Phishing Attacks Based on Discriminative Key Point Features of Web" International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (1) : 2012

[15] "Adil Alsaid and Chris J. Mitchell" "Preventing Phishing Attacks Using Trusted Computing Technology" Information Security Group, Royal Holloway, University of London Egham, Surrey TW20 0EX, UK

[16] "Peter Finn Markus, Jakobsson" "Designing and Conducting Phishing Experiments".

[17] Federal Bureau of Investigation. Spear phishers .http://www.fbi.gov/news/stories/2009/april/spearphishing_040109.

[18] "Cryptography & network security" Principals and practices Third Edition Pearson education 2003, William StallingISBN:81-7808-902-5. www.verisign.com.au/repository/tutorial/digital/intro1.shtml

[19] Identity thieves take advantage of voip. http://www.icbtollfree.com/article_free.cfm? ArticleId=5926.

[20] Mark Hughes (4 January 2008). "Logos that became legends: Icons from The independent, http://www.independent.co.uk./news/media/logos-that became-legends-icons-from-the-world-of advertising-768077.html. Retrieved 2008-04-27.

[21] "Cryptography & network security" Principals and practices Third Edition Pearson education 2003, William Stalling ISBN: 81-7808-902- 5.

[22]www.verisign.com.au/repository/tutorial/digital/intro1.shtml

[23] https://www.sfbay-infragard.org/Documents/phishing-sfectf-report.pdf
[24] "Rachna Dhamija & J. D. Tygar "Proceedings of the 2005 symposium on Usable privacy and security Pittsburgh, Pennsylvania, Pages: 77 – 88, Year of Publication: 2005, ISBN: 1-59593-178-3
[25] Spear Phishing' Tests Educate People about Online Scams, by Wall Stre Et Journal, http://online.wsj.com/public/article/SB112424042313611531 8jLB2WkfcVtgd8jLBAWf6LRh733sg_20060817.html?mod=blogs 17- August 2005.
[26] Protecting People from Phishing: The Design and Evaluation of Embedded Training Email System, http://www.cylab.cmu.edu/files/pdfs/techreports/cmucylab06017.pdf, November 9, 2006 CMU-CyLab-06-017
[27] "M.Bellare, D.Pointcheva, and P. Rogaway" "Authenticated key exchange Secure against dictionary attacks" Proceedings of Euro crypt 2000.