ISSN:0975-9646

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

Anti-Phishing Design Using Mutual Authentication Approach

Mitesh Bargadiya[#1], Vijay Chaudhari[*2], Mohd. Ilyas khan[*3], Bhupendra Verma[*4]

[#]*PG Research Group (M.Tech IV Sem), IT-Department, RGPV*
Technocrats Institute of Technology (TIT), Bhopal (M.P.) INDIA
[1]miteshbargadiya@gmail.com

[*]*PG Research Group, IT-Department, RGPV*
Technocrats Institute of Technology (TIT), Bhopal (M.P.) INDIA
[2]vijay_ashish@yahoo.com
[3]mikbpl_2003@yahoo.co.in
[4]bk_verma3@rediffmail.com

Abstract—
T*he 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. We recommend an approach, "anti-Phishing Design using Mutual Authentication Approach" With mutual authentication, a connection can occur only when the client trusts the server and the server trusts the client. The exchange of data is carried out by means of the Security protocol. For the anti-Phishing system we are proposed mutual authentication protocol & hash generating function RIPEMD-160 along with one time password. Our process can efficiently reduce the risk of phishing in very simple steps to naive computer user.*

Keywords- Anti-Phishing, Client-Server Authentication and RIPEMD-160.

I. INTRODUCTION

In this paper, we are discussing about Client-Server Authentication for anti-Phishing Design in the context of phishing attacks. 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. Phisher generally wants to know about personal or Financial information such as user name, spouse name, date of birth, account No., credit card No, contact No., as well as ID & Password.

Number of unique phishing web site detected in the year 2009: October 46522, November 44907 and December 46190. Number of brand hijacked by phishing campaigns in year 2009: October 356, November 306 and December 249 [1].

It should be noted that from last few years, Financial Services category remain on first position of most targeted industry sectors science APWG began tracking the proportions of phishing attack but in 2009 first two quarters ranked by Payment service category[1].

In the United Kingdom losses from web banking fraud—mostly from phishing—almost doubled to £23.2m in 2005, from £12.2m in 2004[2] & United States businesses lose an estimated US$2 billion per year as their clients become victims. In 2007 phishing attacks escalated. 3.6 million citizens lost US $ 3.2 billion in the 12 months ending in August 2007[3].

In the second section of the paper we analysis the pervious proposed system and discuss some properties of them.

In the third section we are performing problems analysis related to secure communication (phishing). In the fourth section we propose a novel technique "anti-Phishing Design using Mutual Authentication Approach". Finally we present the Conclusion & future works with the references.

II. DEFENSE BELONGINGS

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[4]. 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. [5]

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 certificate is 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 [6].

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 behavior 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.

III. PROBLEM ANALYSIS

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 [7]. Client can not correctly determine the domain name of the website page with URL https://www.icicionline.com /dsw?psw/index12365 was 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 [8].

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[9].

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 [10].

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[8].

E. Some Common Attacks

Dictionary Attack usually known as Passive Attacks, Phishing sites find a hash of the user’s password that can be vulnerable to a dictionary attack. How do we reduce the effectiveness of dictionary attacks [11]. A dictionary attack consists of trying "all word in the thesaurus" as a possible password for an encrypted message.

Brute force attack is used to crack the encryption of information. It searches the possible keys until correct key is found. The selection of a proper key length depends on the practicability of the stage a brute force attack. By complicate the data to be encrypted; brute force attacks are less efficient as it is more complicated to breaking the encryption.

Another type of attack, Hijack Attack is a form of active wiretapping in which the attacker snatches control of an earlier established communication session. In accumulation to the exchange, the hacker may change the messages to both parties, which results the Man-in-the-Middle attack. This reduces the risk that an attacker could simply guess a valid

session key through trial and error or brute force attacks, Use long random number or string as the session key.

A replay attack is a type of network attack in which a legitimate information communication is maliciously or fraudulently repeated or tardy. This is carried out either by the originator or by a challenger who seizes the information and retransmits it, possibly as part of a masquerade attack by IP packet substitution [12].

In a classical collision attack, the attacker has no control over the content of either communication, but they are at random selected by the algorithm. Mathematically assured, a collision attack finds two different messages m1 and m2, such that hash (m1) = hash (m2).

An addition of the classical collision attack is the chosen prefix collision attack. In this case, the phisher can choose two randomly different data, and then attach dissimilar calculated values that effect in the whole data having an identical hash value. This attack is much more influential than a classical collision attack. Mathematically stated, given a prefix p, the attack finds two dissimilar appendages m1 and m2 such that hash (p || m1) = hash (p || m2) [13].

F. Secure Socket Layer Identification

If client can constantly identify a genuine SSL padlock icon on the status bar, they may be confounded by what that padlock really means. The padlock icon signifies that the site, client is surfing was delivering to the client securely [14].

However, in the case of non-SSL protected web pages, security indicator is missing. Many users do not notice the absence of an indicator.

G. SSL Certificates with Brand Name

Most clients have no information of certificate authorities (CAs) and what belief in a CA involves. Though users can specify the CA's that they trust to sign certificates, very few of even the most sophisticated users take checking step [15].

We found that approvals from Verisign were taken most significance. Approximately every client talking about Verisign by name as a positive factor in, their trust evaluation. Safe-site, Thawte Consulting (Pty) Ltd. and KL-Detector approval had less significant effect.

IV. PROPOSED SOLUTION

For the anti-Phishing system we are proposed mutual authentication protocol using hash generating function RIPEMD-160 which is RACE Integrity Primitives Evaluation Message Digest (RIPEMD-160), 160-bit message digest algorithm developed by Hans Dobbertin, Antoon Bosselaers and Bart Preneel at the COSIC research group and first published in 1996. It is an improved version of RIPEMD, which in turn was based upon the design principles used in MD4, and is similar in performance to the more popular SHA-1. RIPEMD-160 was designed in the open academic community & not known to be constrained by any patents [16].

In our system we are assuming that user must present physically to complete some formalities such as give some welcome messages like "You should be working", "Save the Earth" etc. for the server generated user screen, must submit or select some images, to create random generated graphics password and select five questions & give the answers in one word. User must provide personal mobile number for secure one time password receiving agent. After completing the formalities user receives a unique User Identification Number (U_ID) for the initial steps in the login. Finally user selects an alphanumeric eight digit password (U_KEY) as Final Password.

Now we are presenting the novel method "Mutual Authentication Approach for anti-Phishing Design".

Some important steps are below:

Step 1 C: [U_ID + Req_S_Auth]

Step 2 S: [Resp_S_ID + U_SD]

Step 3 C: [Resp_U_SD + Req_M_Key]

Step 4 S: [Resp_M_Key + U_SD]

Step 5 C: [M_Key + U_Key]

Step 6 S: [Acknowledge to C]

Above notation are given only for overview purpose, the actual communication is secured by Mutual Authentication & RIPEMD-160.

In the first step user enter the unique User Identification Number to start communication with the server and request the server's identity (Req_S_Auth).

In the second step, Server verifies the User Identification Number from the database. If U_ID verified then server elect some entity from previously submitted data (U_SD) and configure a query for the user to prove the identity.

In the third step client receive the query which contain four segments, first segment show the "welcome message-1" to authenticate the server & offer the user to choose one previously submitted question from the question pool and user must give the correct answer to prove user's identity, the remaining three segments are used to generate graphics password, each segment containing one submitted image mix with other images now user must provide its legitimacy by electing the one correct image from each segment. User proves authentication & request to the server to send one time password (Req_M_Key).

In step four, Server checks the response of step three, if found valid then sends the one time password on the user

mobile number (Resp_M_Key) and sends the "welcome message-2".

In the step five, Server again provide own identity by showing "Welcome Message-2" and enquire for the User Final Password with one time password received on mobile.

In step six, Server verifies the both passwords and send positive acknowledgement to the client and allow him to access the resources.

V. CONCLUSION & FUTURE WORK

In this paper we perform an analysis of the phishing and the line of attack in which it affect the client & association. 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 we can use stronger Encryption & Decryption Algorithms, Hash Function algorithms and Mutual authentication framework with Genetics algorithms & Biometric Password to improve the overall security of communication.

REFERENCES

[1] http://www.antiphishing.org/reports/apwg_report_Q4_ 2009.pdf
[2] http://www.finextra.com/fullstory.asp?id=15013, Finextra. March 7, 2006
[3] http://www.gartner.com/it/page.jsp?id=565125. McCall, Tom December 17, 2007.
[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] "Cryptography & network security" Principals and practices Third Edition Pearson education 2003, William Stalling ISBN: 81-7808-902-5.
[6] www.verisign.com.au/repository/tutorial/digital/intro1.shtml
[7] http://www.sfbay-infragard.org/Documents/phishing-sfectf-report.pdf
[8] 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
[9] 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.
[10] Protecting People from Phishing: The Design and Evaluation of Embe-dded Training Email System, http://www.cylab.cmu.edu/files/pdfs/tech_ reports/cmucylab06017.pdf, November 9, 2006 CMU-CyLab-06-017
[11] M.Bellare, D.Pointcheva, and P. Rogaway. Authenticated key exchange Secure against dictionary attacks. Proceedings of Euro crypt 2000.
[12] http://en.wikipedia.org/wiki/Replay_attack
[13] http://en.wikipedia.org/wiki/Collision_attack
[14] Oppliger, R. Hauser, R. Basin, D. SSL/TLS Session-Aware User Authentication Issue: March2008, Volume: 41, Issue: 3, On page(s):59, ISSN: 0018-9162.
[15] R. Dhamija, J.D. Tygar, M. Hearst, "Why Phishing Works," In the Proceedings of the Conference on Human Factors in Computing Systems (CHI2006), 2006
[16] http://homes.esat.kuleuven.be/~bosselae/ripemd160.html