COUNTER CHALLENGE AUTHENTICATION METHOD: A DEFEATING SOLUTION TO PHISHING ATTACKS

Cheman Shaik

VISH Consulting Services Inc, 6242 N Hoyne Avenue, Chicago IL 60659, USA

ABSTRACT

A counter challenge authentication method is presented for authentication of online users of web applications. The authentication method involves a counter challenge from a user to a web application asking to provide certain information from one or more user details recorded at the time of registration. The user enters his password and logs into the web application only in case the correct answer is received from the web application. This advanced authentication method protects online application users from phishing attacks. An incorrect answer or inability of the web application to provide the correct answer to the challenge is a clear indication of a phishing attack, thereby alerting the user and stopping submission of password to phishers. The authentication method is computer independent and eliminates dependency on two-factor authentication, hardware tokens, client software installations, digital certificates, and user defined seals.

KEYWORDS

Phishing Attacks, Counter Challenge, Social Engineering.

1. INTRODUCTION

Phishing is a kind of attack mounted through a spoofing spam that causes serious data or financial losses to consumer based online businesses. In phishing attack, a fraudulent mass email is sent to a huge count of users, impersonating a target organization with a message to update their personal information such as User Id and password related to a web application, failing which their accounts will be deleted or access to the concerned web application will be blocked. The reason for the sudden requirement of updating personal information is often stated in the phishing mail by the attacker as some enhancement of security applications that has taken place on the web server. Unaware of the trick, many times users submit their personal information, which is directed to a fraudulent server owned by the attacker. Once the attacker captures the personal information, it will be used for fraudulent transactions with the web application. Sometimes, the personal information that a phisher asks for may also include credit card, social security, and bank account numbers.

Phishing attacks usually target users of online banking, payment services and e-commerce sites. Many of the major banks across the world fell victim to phishing attacks at least once. Phishers develop a login web page that exactly resembles that of a target organization, including the logo and images, and send it to target users in an email message, asking them to login immediately to keep their accounts active. Sometimes, they send an email only with a link to the login page that they host on their fraudulent server. Most of the times, the login page is hosted at a URL (Uniform Resource Locator) that mostly matches with that of the

DOI: 10.5121/ijcsea.2020.10101

original, genuine login page, except with a slight difference in the domain name, which is rarely spotted by users.

The consequences of a phishing attack for an online business include direct financial losses caused by fraudulent transactions performed with the stolen information, loss of reputation and customers, customer law suits, fall of shareholder value, and unexpected expenditure to meet post-attack requirements as per federal regulations.

2. AVAILABLE SOLUTIONS

Phishing has no perfect, simple solution as it is more a social engineering problem than a technical one. An early approach to contain phishing attacks involved user education with guidelines such as for not responding to emails asking for any personal information, verification of URLs while furnishing login credentials in any web page, and verifying IP (Internet Protocol) address of the sender of phishing email. However, despite the above approach, phishers continued to be successful in targeting online web application users and stealing valuable personal information.

Utilizing a URL masking vulnerability of the Internet Explorer browser discovered in 2003, phishers used to cheat web application users and steal their personal information. Later, in the wake of growing phishing attacks, some commercial service companies emerged in the market, with a service offering to constantly monitor a domain name system, and registrars to spot domain names that spell closer to existing domain names and are used to launch duplicate websites to cheat customers. As and when such counterfeit domains are identified, the original domain owners are informed of the potential threat. Also, anti-spam service providers offered to scan emails for potential phishing attacks and report them to the targeted companies. However, these approaches are reactive in nature and can only lower the impact of a phishing attack by alerting a company of phishing attacks already in progress.

Two-factor authentication is another approach introduced by product-based security companies. This approach requires that users of an online web application use a second factor of authentication such as a hardware token or smart card provided by the application owner. After a user submits his login credentials for authentication, the web application further prompts him to enter a number that his hardware token generates or enter his smart card in the reader slit of his computer. Though this approach provides a definitive solution to phishing attacks, it carries its own disadvantages such as high hardware token cost, client software installation, high management costs and user education requirements.

Unfortunately, hackers have become successful even in defeating two-factor authentication by creating a phony process to both phish victim's passwords and the special two-factor authentication code [1].

Another approach to spotting phishing attacks is comparing a mail server IP address with the email sender's domain name[2]. However, the email sender's domain name can be spoofed to fool users, and the comparison task is not easy for a layman without much knowledge of domain names and IP addresses. One more approach that has been tried by corporations to contain phishing attacks is digitally signed emails wherein the sender attaches his digital signature to his email[3]. However, as a phisher also could have digitally signed with his valid digital signature, it requires that the email recipient verify and identify the phisher's misleading domain name.

Some banks have their own solution to phishing attacks. A user of their web application can select a seal that will be displayed on the login page whenever the login page is displayed. However, the seal appears only on the computer that is used to select the seal. When the user switches to another computer, the seal management application would not be able to detect the user and identify a corresponding seal.

A browser plugin named *Antiphish*keeps track of sensitive information and warns users when sensitive information is entered in web pages. However, AntiPhish flags even legitimate re-use of credentials as suspicious and is therefore not reliable [4]. Similarly, *SpoofGuard*is another browser plugin that examines webpagesandwarnsuserswhenwebpageshaveahighprobabilityofbeingspoofs, based on their URL, images, and links. However, *SpoofGuard* checks can be evaded by simple modifications to spoof pages[5].

Many browsers have in-built defending mechanisms through active or passive indicators against phishing sites. Active indicators throw warning popups against suspicious sites whereas passive indicators do not interrupt users and are less effective [6]. Some times even active indicators fail to work if a user disables popup in his browser.

The shortcomings of all the solutions discussed above to defeat phishing call for a more simple, technical, computer-independent solution to phishing, without demanding additional hardware, software, and education on the part of end users.

3. COUNTER CHALLENGE AUTHENTICATION

Counter Challenge Authentication is an efficient approach to contain phishing attacks. It provides a simple, computer-independent, technical method for defeating phishing attacks, without requiring any education on the part of users.

The method utilizes a user challenge to the authentication server prior to authentication in order to overcome the phishing problem. As it is clear to web application users, authentication is a process wherein a web application verifies if a user is registered and holds an account on its systems. In order to meet the challenge, a user enters his User Id and Password in a login page and submits it to the web application. Subsequently, the web application verifies if the user credentials received already exist in its user database. If the verification proves the user is already registered, access is allowed to the web application, else access is denied. This mechanism of straight authentication was developed in the early stages of web technology when no one could foresee phishing attacks as a daunting future problem. Today, this straight authentication mechanism has proved inefficient to thwart phishing attacks.

Counter challenge authentication is an advanced authentication method enabling users to safely login to web applications, without falling prey to phishers. In this method, a user poses a counter challenge to a web application through a challenge page displayed in his browser. A simple challenge page as shown in Fig. 1 may comprise an input box for User Id, a message below the input box asking the user to pose a challenge by requesting certain information from his personal details corresponding to the selection of certain input elements displayed on the web page.

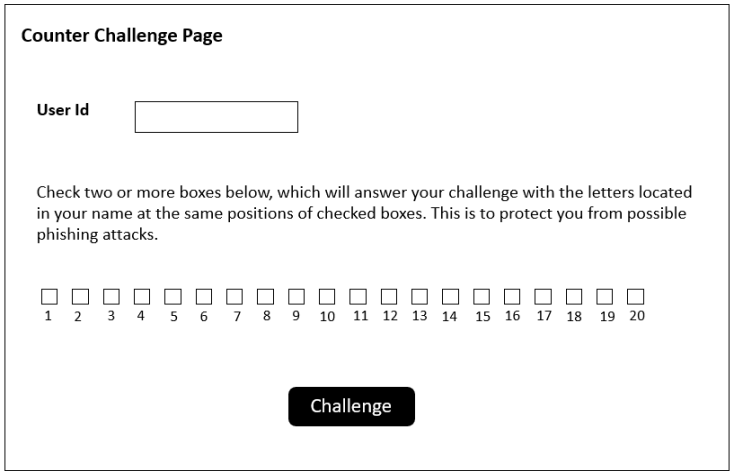

Fig.1. A counter challenge page used in authentication process

The input for a challenge may be provided by checking one or more of a set of check boxes available on the challenge web page as shown in Fig.2. In a generic sense, input may also be provided by selecting items from a number of drop-down lists, clicking a number of buttons, filling one or more input boxes or clicking one or more images available in the challenge web page. The selected items, clicked buttons, images, or the information filled in the boxes represent the characters or values that the user requests from the web application.

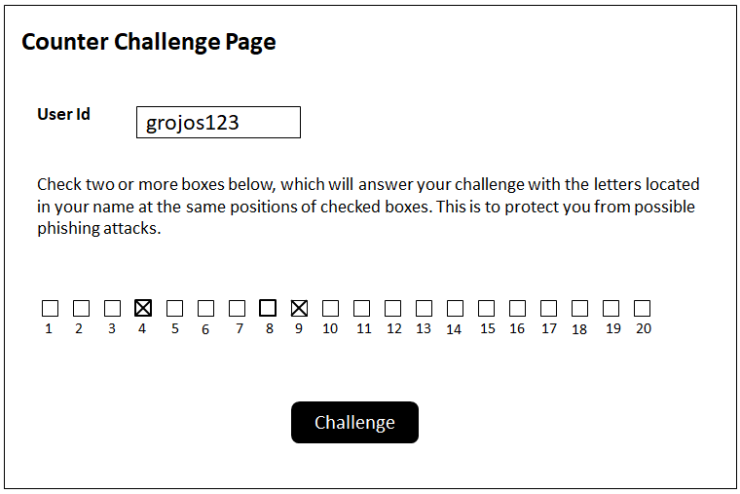

Fig. 2**.** A counter challenge page with user input

The web application will return in response the letters or values as requested from the user's personal details. For instance, if a user checks the 4th and 7th check boxes in the set of check boxes representing the user's name, the response from the web application will return, as shown in Fig. 3, the 4^{th} and 7^{th} letters from the user's name as registered with the web application, in an email to the user's email address or to his mobile phone.

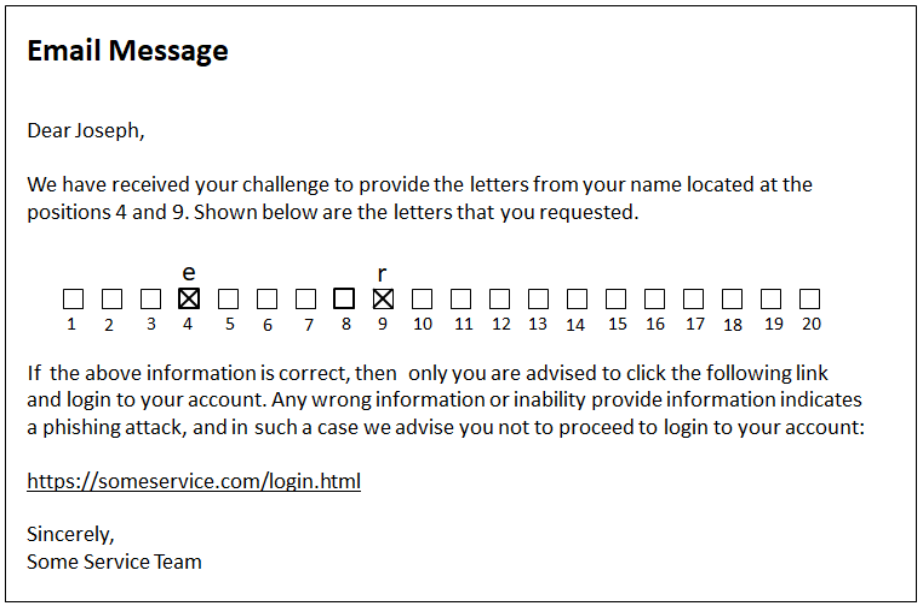

Fig. 3. A message sent to a user's email address in response to the user's challenge

The message in the email or to the mobile phone advises the user to proceed to login only in case the answer provided to the challenge is correct. The email message sent to the user comprises a link to the safe login page as shown in Fig. 4 which the user is supposed to click only if the answer provided is correct. When a message is sent to a user's mobile phone, the user is supposed to verify the correctness of the answer and then enter the user's password in a web page which could be the same web page used for counter challenge or a different one.

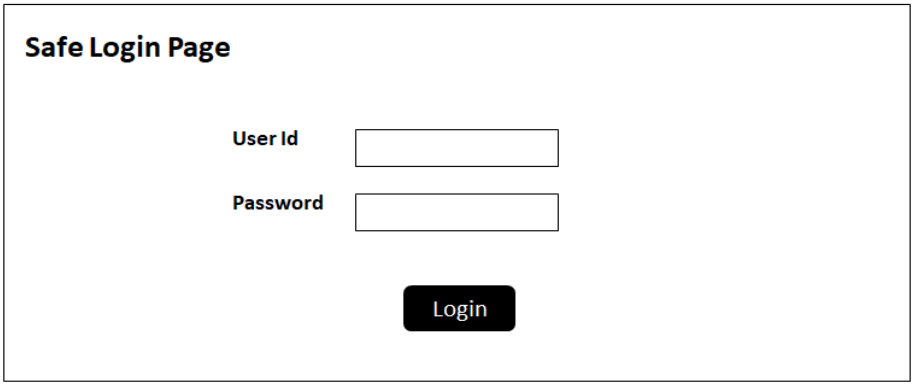

Fig.4. Asafe login page displayed after answering a user's challenge

The counter challenge page may also provide an option as shown in Fig. 5 as to where the answer to the challenge needs to be received. The user may indicate his choice as email or mobile phone through a couple of radio buttons or similar user interface elements provided in the challenge page.

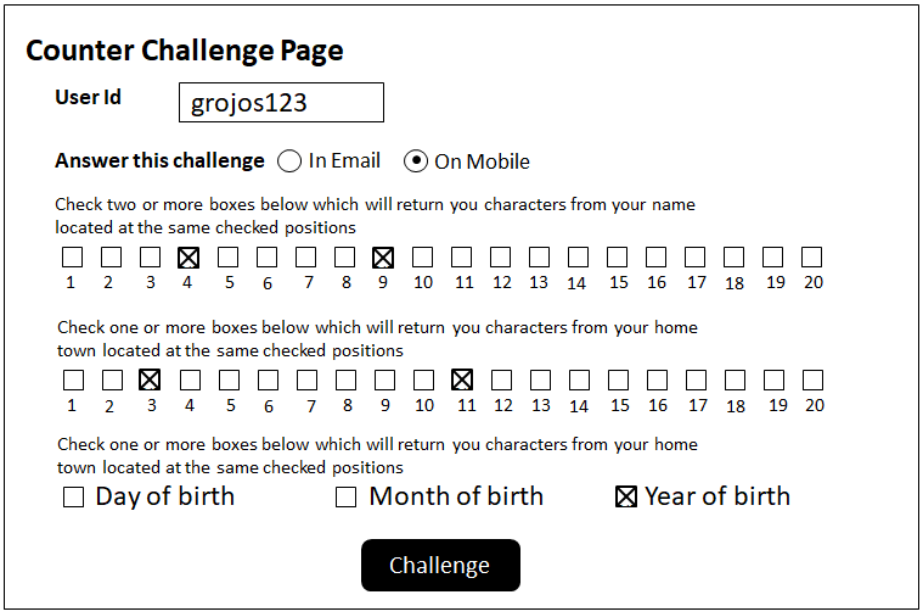

Fig.5. A counter challenge page with email and mobile options to receive answer

The concept of counter challenge by a user before login and providing an answer by the authenticating web application to the counter challenge protects a user from phishing attacks as the user refrains from submitting his password, in case the web application fails to provide the correct answer. A phisher's fraudulent web application will be unable to correctly answer a user's challenge as it lacks the required information to meet the challenge. Any failure to respond to user's challenge or incorrectness of response is a clear indication of a phishing attack. Only the genuine web application can answer the user's challenge as it has all the user details captured and stored at the time of registration. This simple technique of counter challenge authentication inherently includes a defeating mechanism against phishing attacks.

4. IMPLEMENTATION

Counter challenge authentication can be implemented in a single login page also using AJAX (Asynchronous JavaScript and XML) and DHTML (Dynamic Hypertext Markup Language). In such an implementation, the login page comprises an input box for user id, a series of check boxes or other input elements, and a "Challenge" button in visible form. Another input box for password and a Login button are also embedded in the same login page in hidden form. A user enters his user id, selects some check boxes or input elements available in the login page, and then clicks the "Challenge" button. The web application responds to the challenge in the same page with the correct answer, and at the same time the hidden password box and the Login button are made visible on the web page, while hiding the Challenge button. The web application also displays a message on the same login page to enter password only if the answer to the challenge is correct.

5. ADVANTAGES

An advantage of a counter challenge authentication method is it does not require any user education, and it only requires that users read the messages and act accordingly during the process of authentication. Users automatically get educated and used to counter challenge authentication as its look and feel is entirely different from the traditional login pages. Users easily conceive what they are doing, what is happening and what they are supposed to do in order to avoid phishing attacks.

Another advantage of this authentication technique is it is computer independent, unlike a user-seal based solution to phishing. It enables users to login to their accounts through any computer, irrespective of its IP address and geographic location, thereby eliminating dependency on one's own personal or regular usage computer.

Further, this authentication technique eliminates dependency on client software installations and digital signatures. Counter challenge authentication works as an alternative to expensive hardware tokens, thereby avoiding cost and maintenance issues. Post attack panic and cost of meeting legal procedural requirements can be avoided with this technique.

The method of counter challenge authentication can be used in many other ways than the one described above. Instead of requesting letters from a user's name, they can be requested from other details of a user, such as the user's mother's maiden name, university of graduation or any other personal detail that was furnished and stored in a user database at the time of registration. Further, to make the request of letters complicated, a user may be enabled to request letters from different chunks of user details.

6. NUMERICAL ANALYSIS

The possibility of a successful phishing attack on users of a web application with counter challenge authentication by answering challenges with random letters or values has been studied. The study reveals that the chances of success for such a smart phisher are negligible when the number of requested letters is two, and gets close to zero as the number increases. The following table shows the probability figures of a phisher's success with respect to the number of letters requested in the challenge of authentication.

Table1. Probability figures of successful phishing attack

Number of requested letters	Probability of successful phishing attack
2	$1/26^2 = 0.00148$
3	$1/26^3 = 0.00006$
4	$1/26^4 = 0.000002$
5	$1/26^5 = 0.000000084$

The above figures were calculated based on the assumption users' names are always permutations of 26 letters of the English alphabet. However, numbers, period, white space and uppercase letters are not considered in computing the above figures, which, if considered, may further curtail the chances of success.

7. LIMITATIONS OR DEFICIENCIES

The proposed method and solution to phishing attacks does not suffer any limitations or deficiencies in implementation. The implementation is simple, easy and straight forward. The only resistance by the user community is the method's deviation from the age-old, traditional login method that allows login with a single button click. However, the user community will get accustomed to the new login method in a very short period as they well understand and realize its benefits.

8. RECOMMENDATIONS FOR FUTURE WORK

The solution discussed to defeat phishing attacks uses data provided by users at the time of registration. The concept and method are illustrated with the help of the most common data such as users' name, address, date of birth etc. For future work it is recommended that a vast, detailed survey may be conducted on the different types of data collected by online web application during registration and probability figures of successful phishing attacks may be computed for all possible combinations thereof.

9. CONCLUSION

Counter challenge authentication methodis a definite, technical solution to phishing attacks and will be very useful for e-commerce applications, e-banking systems, email and web hosting services, and all other web applications that require user authentication. Once implemented by online applications and adapted by users, it saves even laymen from falling prey to phishing attacks as it does not require any user education.

REFERENCES

1. Mashable webpage, https://mashable.com/article/hackers-beat-two-factor-authentication-2fa-phishing/, last accessed 2019/12/29

2. Univ. of Texas webpage, https://identity.utexas.edu/everyone/spotting-a-phishing-email, last accessed 2019/12/29

3. GlobalSign webpage, https://www.globalsign.com/en/blog/how-to-spot-a-phishing-email/, last accessed 2019/12/29

4. Dr. Radha Damodaram: Study on Phishing Attacks and Antiphishing Tools. International Research Journal of Engineering and Technology (IRJET)3 (1), 700-705 (2016)

5. Rachna Dhamija, J.D. Tygar: Human Interactive Proofs to Detect Phishing Attacks. In Human Interactive Proofs: Second International Workshop (HIP 2005), eds. H. Baird and D. Lopresti, Springer, May 2005, pp. 127-141

6. Ike Vayansky and Sathish Kumar:Phishing – challenges and solutions.Computer Fraud & Security. January 2018, pp. 15-20