# An Evaluation of Page Token in OpenID Single Sign on (SSO) to Thwart Phishing Attack

Nur Haryani Zakaria, Mohd Faizal Zainul, Norliza Katuk, Hatim Mohammad Tahir, and Mohd Nizam Omar
*School of Computing, College of Arts & Science, Universiti Utara Malaysia, Sintok, Kedah, Malaysia*.
*haryani@uum.edu.my*

***Abstract*— Single Sign-on (SSO) was introduced to overcome the issue of password memorability among users as researches have shown that users struggle to cope with too many sets of password as number of account increases. This is due to SSO relies on the usage of single authentication that allows users to access to multiple websites or services. As much as it has managed to solve the memorability issue to certain extend, users were found to have skeptical in its adoption due to security concerns. Among common issues of SSO is that it is prone to several attacks like spam, link manipulation, session hacking and particularly phishing. Despite of many efforts been placed to overcome phishing attack with regards to SSO, the effectiveness of the proposed solutions are yet to be proven by conducting extensive evaluation. Thus, this study intends to conduct an evaluation on a particular solution of phishing attack call page token. Page token was proposed recently which was claimed to be able to mitigate the issue of phishing attack with regards to SSO application. The evaluation involved a control laboratory experiment with participants being recruited to experience the usage of page token as a protection mechanism against phishing attack. The results showed are promising along with several suggestions given for further enhancement.**

***Index Terms*—OpenID; Page Token; Phishing Attack; Phishing Tool; SSO.**

## I. Introduction

Nowadays, security measure is an important aspect for preventing and protecting the confidentiality of data. Recently, Single Sign-on (SSO) was introduced to replace conventional authentication method that is said to solve the issue of password memorability. According to Open Group, SSO is a protocol that requires single action of user authentication that can granted a user to get access for all systems and services where users get permission to access with the usage of only one password rather than multiple passwords [1]. There are some protocols that have been used in SSO such as Keberos, SAML, OpenID, OAuth and Inforcard. However, this study will focus on OpenID since it is the most commonly used protocols in SSO. Some web services are using OpenID as their security tools such as Microsoft, Symantec, Google and Verizon [2].

The introduction of this SSO was claimed to release user's burden from memorizing many usernames and passwords for different account. According to password habit study on password memorability, a typical account holder has about twenty five different accounts that require different sets of usernames and passwords thus the effort to memorize password is really a huge challenge [3]. This study also estimated that a user has to type eight different passwords per day and this situation creates an extra burden on user especially when it comes to managing password efficiently.

Despite of its advantages in reducing users burden to memorize passwords, this OpenID protocol has several known vulnerabilities. Among the most common is that it is prone to phishing attack [4]. Researchers in [5] revealed that phishing attack in OpenID is also possible to happen even when Secure Sockets Layer (SSL) is in operation. A research by [6] also supported the claim that SSO is also prone to session hijacking and phishing attack. When further research is done on this phishing attack, it was discovered that one of the possibility that this phishing attack becomes common is due to the availability of phishing tools to be manipulated in the market. In the context of OpenID, the phisher will take username and password and they can act as a legitimate user and will get full access and control from the system. Due to this situation, phisher will take advantage and able to manipulate this limitation of memory problem.

## II. Literature Review

Many security issues on OpenID have been reported with regards to the implementation of SSO such as single credential, hijacking and phishing. One of the most common issues that have been raised in OpenID is phishing which is due to the advancement of phishing technologies and techniques. It had caused many financial agencies to have loss billions of money either consumers or e-commerce companies. Alrodhan & Alqarni [7] reported that phishing attack is one of the major security issues with regards to OpenID because of the lack of documentation of the OpenID. OpenID standards are rapidly gaining adoption on the Web and they enable over one billion user accounts. However, the large scale for phishing attack to SSO systems has been significantly underestimated.

According to the Anti-Phishing Working Group (APWG) first half 2017 report [8], the total number of phishing that quarter year was reported at 50, 720 involved the top three countries like United State, Brazil and Ireland with 1269, 475 and 221 cases respectively in the month of June 2017. It involved of several major industries due to the availability of phishing tools and techniques that requires minimal effort from the attackers to manipulate its usage in order to gain access to user IDs and passwords thru fake websites.

There are several solutions that have been proposed to overcome the issues of phishing attacks in OpenID. One of the most common is relying on user awareness [9]. However this approach is very challenging as users are known to be the weakest in the link when it comes to security. They are easily manipulated as always regarded security as secondary tasks and will prioritize their main agenda over security without hesitation. This makes user awareness approach the least preferable solution. Moreover, with the advancement of

technologies these days, tools to generate phishing attack are readily available in the market which is among the factors that increases phishing attacks.

The Secure Socket Layer is another solution [10], which was proposed to protect and secure OpenID protocol. However, SSL is not sufficient to protect OpenID protocol from being compromised. The key issue with SSL is when user's lack of security knowledge. Attackers can manipulate this weakness as most users seldom know how to verify the SSL certificates in the web browser and acquaint the details presented in the certificate. In other words, when the solution requires technicality, it may be too complicated for users to rely on as effective protection mechanism.

Other solution such as nonce and cookies [11] are usually set as default security. The nonce work if user is the first one to use OpenID identifier. However, fast attacker who is sniffing the communication channel can obtain the URL and reset a user Transmission Control Protocol (TCP) connection and steal the user session ID. There are also solutions that attempt to combine nonce with cookies. One time cookies (OTC) generate one token per request that is unique using Hash-based cookies Message Authentication Code (HMAC), which provides the prevention from the attackers to steal a session ID. However, the usage of OTC is limited since it is only available with WordPress OTC plug-in and OTC extension for Firefox only.

Browser's fingerprint [12] is an approach that user does not need to change underlying user browser and can use the initial authentication process to build further security measurement. It will register the user browser and user system (i.e., operating system and system architecture) when user request service. Web server will reset the connection if it identified. However, it has limitation because the HTTP headers and their ordering as well as user browser and can be set arbitrarily. Furthermore, browser's fingerprint has complex architecture. All existing solutions as discussed above do not solve the phishing attack totally and still have their own limitations. In order to overcome the phishing problem, page token was introduced recently as a mechanism to thwart phishing attack.

This proposed solution was inspired by research in [13] whereby it is implemented as double factor authentication. Similar to other proposed solutions, page token requires an extensive evaluation to demonstrate its true capability as protection mechanism towards phishing attack. Thus, this study will conduct an evaluation of page token as protection mechanism against phishing attack in OpenID SSO. The next section will elaborate further on the implementation of page token with regards to this study.

## III. PAGE TOKEN IMPLEMENTATION

Page token refers to a mechanism which acts as a second authentication after logging to the system in order to allow user to proceed further using the system. Page token will be generated by IdP (Identity Provider) by using combination of one-time random password and encrypted page token for user machine identification. This approach was used for an alternate email address or short messaging system (SMS) where user will retrieve the one time password (OTP) and will expire after single use [14]. The IdP generates page token that will be send to user based on registered email or mobile number and then it will send authentication protocol simultaneously to user for authentication reason [15]. User must send the page token to RP (Relying Party) to validate the user – whether they are legitimate or not. If the page token matched then the user will be granted to use the system - otherwise, the user will be blocked and the system will recognize that as phishing attempt. By embedding page token into OpenID, if the phisher or attacker got ID and password, they will be able to login to the system only. They are not able to do any activities such as transaction, transferring, copying or deleting that as a part of the functions of the system because any operation of the system must be authenticated by page token. Page token will be sent to the registered hand phone number or email only to receive page token as second credential for user to send to the system.

The existing OpenID has one layer but the OpenID with page token has two layers. These layers help to protect and mitigate from unwanted user that often ignored. The more layers of security applied, the better it is for protection effort. OpenID with page token is said to offer additional security layer as the first layer acts as primary authentication that will detect, deter and delay unwanted access. It also provides a limitation for unwanted user by providing personal audit by system requesting ID and password for user recognition. For second layer as secondary authentication for protecting the further access that restricted by system. User need to request access and system will send page token to user's email and user need to enter the given token to get grant access from system to do any activity in the system. The goal of secondary security layer is to monitor unwanted access and conduct second verification process to confirm the authorized user.

## IV. METHODOLOGY

The methodology of this study consists of five phases. They are identification of problem, developing prototype of the page token, evaluation, analysis and conclusion. This study starts with identification of problem through conducting literature reviews on related research on OpenID SSO and phishing attack. Once the problem has been identified, the next phase is to proceed with the core focus of the study. Since this study intends to conduct evaluation on a proposed mechanism known as page token, a prototype has to be developed.

This followed by the second phase which is developing prototype for page token. The activities involved in this phase are embedding page token to OpenID environment. The Salesforce.com and Google Console Developer were used to build a prototype of page token. An email was used as platform for authentication for Google Console Developer and Salesforce.com. The Page Token was generated and sent via email as second credential to validate user. Once the prototype is ready, the study proceeds to the next phase.

The third phase involved conducting the evaluation where by a control laboratory experiment was used as an approach to evaluate the prototype. The experiment was mainly intended to measure the performance of page token in SSO environment and observe how users cope with the proposed mechanism. The next phase following the experiment is the analysis phase where the data gathered will be analyzed before finally a conclusion and several suggestions can be drawn based on the analysis done.

## V. EVALUATION

This study aims to evaluate the page token as countermeasure in thwarting phishing attack. In order to conduct the evaluation, control laboratory experiment was used to measure the effectiveness of page token. The experiment conducted at one higher learning institution in the Northern region of Malaysia involving a total of 26 participants. The participants were recruited based on voluntarily aspect and they were requested to complete the consent form before participating. A quick briefing was also conducted at the beginning of the session to give all the participants some ideas on how the whole session will be conducted. They were also given an awareness talk to motivate them to participate in the experiment. Out of 26 participants recruited, 18 participants proceeded to the next stage. Note that participants were given total flexibility to withdraw at any time if they feel uneasy of refuse to proceed as to ensure the experiment is totally based on voluntarily aspects. Further details of the experiment are as discuss below:

### *A. The Apparatus*

The prototype worked on Macbook Pro with windows and Mac OS platforms. The laptop has display with13.3-inch (diagonal) LED-backlit glossy widescreen display with support for millions of colors, 2.5GHz dual-core Intel Core i5 processor (Turbo Boost up to 3.1GHz) with 3MB L3 cache, configurable to 2.9GHz dual-core Intel Core i7 (Turbo Boost up to 3.6GHz) with 4MB shared L3 cache, 4GB of 1600MHz DDR3 memory and 500GB 5400-rpm hard drive. The reasons phishing technique was tested on these platforms to fulfill availability and validity in thwarting phishing attack in cross platform. This apparatus was used to attack participants account as victim by phisher.

For phishing experiment, participants used Hewlett Packard (HP) and Samsung Chromebook. The HP notebook with features such as Windows 10 Home 64, Intel® Pentium® N3700, 29.5 cm (11.6") diagonal HD touchscreen, 4GB RAM with 1TB storage and B&O PLAY with 2 speakers. The second was Samsung Chromebook futures with a 11.6-inch screen; lighter and thinner; and very different under the hood. The Samsung Chromebook uses a low-power processor, Samsung's Exynos 5 Dual, which is built on ARM's new dual-core system-on-a-chip Cortex A15 design (prior versions used Intel Atom and Celeron processors). It also has just 2GB of system memory. Two extended monitors were connected to the both notebook heading to observer for monitoring reason.

### *B. The Procedures*

This experiment used impersonates phishing technique to attack participants as victims. This experiment was to measure the number of successful attack and number of unsuccessful attack. The variable involved are successful attack and unsuccessful attack to be used to measure phishing attack for OpenID without page token and OpenID with page token. For dependent variable involved environment that consist of OpenID without page token and OpenID with page token and the rest are independent variable.

Before the experiment, participants were giving explanation about the awareness, OpenID and SSO. The explanation provided the participants with some knowledge about awareness that related to phishing attack in OpenID and how the phishing works. They were also exposed on how to recognize and make comparison between fake website and the real website and inculcated participants how the best way to react when receive phishing email. At the beginning of the experimental session, participants were divided into two groups; experimental group (i.e.: 9 participants to be tested for OpenID with page token) and control group (i.e.: 9 participants for OpenID without page token). The participants from experimental group were requested to use default email account due to time constraint, while those in the control group are free to use their personal email account.

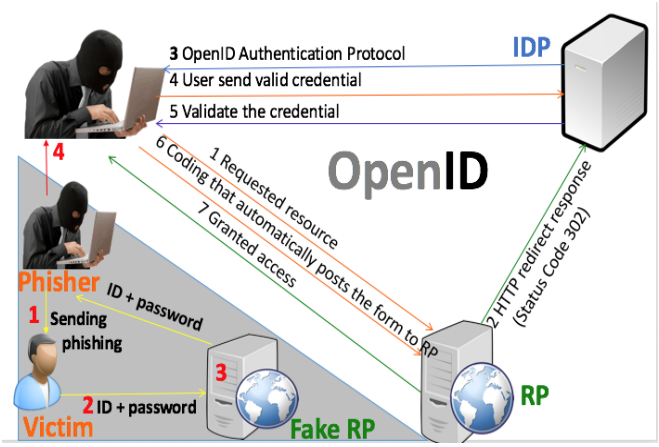


Figure 1: The flow of phishing attack

Figure 1 illustrates the procedures involved in phishing attack. During this experiment, researcher acted as dummy phisher to attack participants as victims by sending phishing email seem as legitimate company's email that provide link to user's email to phish them that aimed to take ID and password. Phisher used AB Bulk Mailer 9.0 for launching attack by using impersonation technique. The email was appealed victims to login to the system for solving problem that somebody tried to get ID and password for stealing reason. The appearance of the fake website that linked to victim's email was same with the original make victims were confidence to do logging. When victims clicked on the given link, it was directed to the fake website. Victims should enter ID and password for updating authentication. They did that action was influenced by important word in title, they had worried about money to be stolen, they feel confidence because the email was sending by Salesforce Company, the email was mentioned about stealing reason if the ID and password do not update. This action will trap victims fall in phishing attack. The entered ID and password will have directed to phisher database. For the next step, phisher will take ID and password and act as legitimate user for attacking the victims account. Data was recorded to be used in analysis.

### *C. Evaluation Metrics*

This study has evaluated page token performance by using security metric to measure the robustness of page token. This evaluation need metric requirement for validating the page token in thwarting phishing attack as metrics below and we explain the preliminary setup of the security metrics experiments. The proposed evaluation security metric to validate the protocol of page token as counter measure that influences the security of OpenID. This experiment proposed to use number of successful logins and number of unsuccessful logins by following Network Security Metrics

Program [16]. The security metrics will describe as follow.

The number of successful logins in one of the metrics being used to refer to successful attack and measured the successful login trial to attack by counting how many time phisher successfully login to saleforce.com for attacking reason. This experiment for this metric measured to OpenID without page token environment and compared to OpenID with page token. If the phisher successful login to the system, this means that the system has been successfully attacked by phisher and the system is not secure enough to be used. This metric presented the total number of successful login. The reason of this metric is to measure the quantity of the number of successful login exposes to the risk phishing attack. There following assumption is used in the experimental setting that is – "*the total number of success trial to login into OpenID authentication system that phisher had to attack to OpenID without page token and OpenID with page token counting as successful logins*". Therefore based on this assumption, the opposite of it will indicate the contradicting positions.

## VI. Findings And Analysis

The performance of OpenID has been evaluated based on without page token and compared to the OpenID with page token by using laboratory experiment as shown in the following metrics below. As mentioned previously, each participant was requested to login to their account. The phishing attack was launched at each individual participant from both control and experimental group. Results in Table 1 showed that those in the attack were more successful in the experimental group compared to control group. This indicates that the page token only managed to mitigate phishing attack to certain extend. Besides that, we observed participants during experiment to see how they cope with the proposed solutions. It was found that only one participant had extra awareness that he did not fall for the phishing attack. There were two participants who only realized that they were phished after they completed the experiment while the remaining of the participants had no idea at all that they were being phished. This observation results indicate that despite the proposed solution, user's awareness still play an important role in mitigating phishing attack.

Table 1
Number of Successful versus Unsuccessful Logins Trial

| Result | Control Group | Experimental Group |
|---|---|---|
| Successful logins (attack) | 8 | 9 |
| Unsuccessful logins (attack) | 1 | 0 |

## VII. Discussion

In this paper, an evaluation has been conducted to measure the performance of page token authentication protocol. The performance was measured based on number of successful logins versus number of unsuccessful logins that indicates successful attack and unsuccessful attack respectively. However, results shown that there is no significant difference between both control and experimental group. Based on our observation, this is probably due to awareness still plays an important role in phishing attack, where user should make decision before clicking any link that was sent via emails. In other words, it also makes phishing easy to work for OpenID environment because phishing rely on social engineering technique that relates to human psychology and difficult to penetrate phishing attack. Furthermore, this is due to sending the page token to email as second credential is not sufficient since phisher has captured ID and password during the first-time login (at phished website). This shows the role of awareness is very important in thwarting phishing attack. Even, based on the observation, during the experiment reveals that victims know about phishing but do not know how phishing works and they failed to realize that they fall as victims. This is a very crucial finding that should be taken into consideration when designing future solutions for mitigating such attacks.

## VIII. Conclusion and Future Work

This study has presented an evaluation of page token by using impersonate technique of phishing attack to determine its applicability as a countermeasure. At the beginning of the research we anticipate that page token will be able to act as a countermeasure to certain extent in thwarting phishing attack. A simple prototype was developed to enable us to conduct an evaluation through a control laboratory experiment. The results indicated that the applicability of page token is strongly accompanied by the user's awareness which highly influences their security behavior.

Based on the outcome of this research, it is recommended that in order for the page token to be more effective, the countermeasure should be sent via short messaging services (SMS) instead of email since the attacker can easily manipulate the phishing victims via email. Alternatively, it could also be more effective if the users supply an additional email as an alternative for sending the page token. These would be our primary focus in the near coming project. In addition, our research team is also interested in investigating further the page token applicability on other types of phishing attack like forward-attack, pop-up attack and voice phishing.

## Acknowledgement

This research was supported by Fundamental Research Grant Scheme (FRGS – S/O Code: 13143) from the Ministry of Education (MoE) Malaysia.

## References

[1] Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems", in 2004 *Proceedings of the 5th Conference on Information Technology Education*, pp. 177–181.

[2] Riesch, P. J., & Du, X. Audit based privacy preservation for the OpenID authentication protocol, in *2012 IEEE International Conference on Technologies for Homeland Security*, pp. 348–352.

[3] Sun, S.-T., Boshmaf, Y., Hawkey, K., & Beznosov, K. (2010). A Billion Keys, but Few Locks: The Crisis of Web Single Sign-On, in *Proceedings of the 2010 Workshop on New Security Paradigms*, p.p 61–72.

[4] Adida, B. BeamAuth: Two-Factor Web Authentication with a Bookmark. *Applied Sciences*, p.p 48–57, 2007.

[5] Unger, T., Mulazzani, M., Fruhwirt, D., Huber, M., Schrittwieser, S., & Weippl, E. SHPF: Enhancing HTTP(S) session security with browser fingerprinting, in *Proceedings of 2013 International Conference on Availability, Reliability and Security*, p.p 255–261.

[6] Muhammad, A., & Tripathi, N. Evaluation of OpenID-Based double-factor authentication for preventing session hijacking in web applications. *Journal of Computers (Finland)*, *7*(11), p.p 2623–2628, 2012.

[7] Alrodhan, W.A. & Alqarni, A.I. Security Investigation and Analysis of OpenID: Problems and Enhancements. *International Journal of Computer Science and Network Security*, vol. 17, p.p 198-211, Oct.

2017.

[8] APWG Phishing Activity Trends Report, October 17, 2017. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_h1_2017.pdf (Date visited: 20th December 2017).

[9] Kirlappos. I. & Sasse, M.A. Security Education against Phishing: A Modest Proposal for a Major Rethink, *IEEE Security & Privacy*, p.p 24-32, 2012.

[10] Krishna, P.V., Misra, S., Joshi, D., Gupta, A. & Obaidat, M.S., Secure Socket Layer Certificate Verification: A Learning Automata Approach, vol. 7 (11), p.p 1712-1718, 2014.

[11] Yalamanchili, S., Rao, M.K. & Chowdary, C.S., Internet Key Exchange Aggressive Mode Negotiation using Cookie & Nonce Alternatives, vol. 2(4), p.p 368-371, 2011.

[12] Kaur, N., Azam, S., Kannoorpatti, K., Yeo, K.C. & Shanmugam, B., "Browser Fingerprinting as User Tracking Technology", in *11th International Conference on Intelligent Systems and Control (ISCO)*, p.p 103-111, 2017.

[13] Tsyrklevich, E., Tsyrklevich, E., Tsyrklevich, V., & Tsyrklevich, V. (2007). Single Sign-On for the Internet: A Security Story. *BlackHat USA, Las Vegas*, 11. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Single+Sign-On+for+the+Internet:+A+Security+Story#0 (Date visited: 20th December 2017).

[14] Huang, X.W., Hsieh, C.Y., and Cheng, Y. C . A Token-Based User Authentication Mechanism for Data Exchange in RESTful API. in *Proceedings of 18th International Conference Network-Based Information System*, pp. 601–606, 2015.

[15] Dacosta, I., Chakradeo, S., Ahamad, M., & Traynor, P. One-Time Cookies: Preventing Session Hijacking Attacks with Disposable Credentials. In *The ACM Transactions on Internet Technology*, *12*(1), p.p 1–24, 2012.

[16] Lowans, P.W. Implementing a Network Security Metrics Program. Retrieved from https://www.giac.org/paper/gsec/1641/implementing-network-security-metrics-programs/103004 (Date visited: 20th December 2017).