Phishing and Abuse of Cookies: Effectivity of Solutions and Security Methods that Prevent Personal Information Exposure on the Web

STUDENT ID: 896522

1 INTRODUCTION

Whether you are simply scrolling through social media, opening emails, online shopping or online banking, the reality is still the same, it is that all users of the internet are still in danger of exposing personal information on the web. This following review of literature analyses and discusses the problems caused by the leakage of information through phishing and abuse of cookies whilst also evaluating the effectiveness of solutions and security methods presently available — concluding that a need for better education in privacy with better implementation of security methods or technologies is crucial towards protecting users.

2 PHISHING

Phishing is a problem (Lam, Chen & Chen, 2008) that induces information exposure by identity leakage, whereby the practice of sending emails containing fraudulent webpage links are used to obtain personal information such as passwords, credit card numbers or social security numbers. This becomes a critical issue to address as emails are sent on a daily basis impacting both consumers and businesses (Sheng, Kumaraguru, Acquisti, Cranor & Hong, 2009). Phishing is also a form of social engineering (Jagatic, Johnson, Jakobsson & Menczer, 2005), as the attacker manipulates individuals by purporting and impersonating a reputable source (Gross & Acquisti, 2005). Furthermore, this enables information leakage from users to become a more intricate problem as research suggests that phishing is becoming more refined and focused towards potential targets, whereby techniques such as "context-aware phishing" (Ragucci & Robila) allow phishers to customise phishing attacks to each user by utilising knowledge of what sites and services each user uses, retrievable via public databases and social networks (2006, Section 2).

2.1 SOLUTIONS

Possible solutions described by Lam et al. is by first configuring privacy settings on online accounts to hide personal information, social connections, and prevent or deny any third party from accessing incoming or outgoing annotations from the user. Secondly, Lam et al. state that the browsing scope of users must be limited to prevent malicious groups from automating the extraction of personal information from users. Thirdly Lam et al. state that each operation containing user information must be validated by the information owner (2008). Another solution is to use anti-phishing tools such as Google Safe Browsing which uses a blacklist of sites associated with identity theft, and, NetCraft Tool Bar which rates the risk of sites relative to the age of its domain (Garera, Provos, Chew & Rubin, 2007).

2.2 DELIMITATION OF SOLUTIONS

Although these solutions are effective they are all limited by a need to raise awareness (Irani, Webb, Li & Pu, 2011) concerning user privacy and involuntary actions that may lead to personal information exposure on the web. Moreover, users must also be educated on the techniques available to prevent information leakage as described by Lam et al. (2008), as well as using anti-phishing tools suggested by Garrera et al. (2007) and control technologies present such as a "Wi-Fi Privacy Ticker" (Consolvo, Jung, Greenstein, Powledge, Maganis & Avrahami, 2010, p. 9). This suggests that a distinction between social engineering and unintentional human errors or deliberate attacks, exists, as explained by Nohlberg (2008), inferring that not only must users protect personal information by technical means but must also aware of potential psychological attacks that may be implemented by phishers.

3 ABUSE OF COOKIES

Although the creation and intended use of cookies by websites, which is to collect and store personal information within a small file, is morally permissible (Lin & Loui, 1998). The manipulation of cookies aid in exposing a user's personal information on the web when a user's cookies are stolen and abused through practices such as cross-site scripting which utilises vulnerabilities found in the procedure of exchanging of cookies between browsers and web servers, in turn, to implement a malicious script, generally directing a user to a phishing page (Takahashi, Yasunaga, Mambo, Kim & Youm, 2013).

The lack of integrity of cookies also has real-world implications (Zheng, Jiang, Liang, Duan, Chen, Wan & Weaver, 2015). For example, visiting websites in open-wireless networks can lead to malicious cookies being injected by an attacker into a user's browser causing their system to become compromised and open to the leaking of personal information, such as browsing history and bank details, whereby an attacker can then "hijack" user accounts in websites like Google, eBay and Amazon, as illustrated by Zheng et al. (2015, pp. 716-718). This infers that the major problem of using cookies to leak personal information is not only caused by communication vulnerabilities but is also caused by uncovered software vulnerabilities in the browser itself, as disclosed by Zheng et al. (2015), identifying how numerous browsers are easily exploitable to the injection of malicious cookies being susceptible to techniques of overwriting and shadowing of cookies are used to violate the integrity of cookies.

3.1 SECURING COOKIES

Cookies can be secured by three types of services which include "authentication, integrity, and confidentiality" (Park & Sandhu). Firstly, authentication processes who owns the cookies by using authentication types that can be addressed-based which collect a user's IP address, password-based which support proxy servers and dynamic IP addresses, or be digital-signature-based which generate cookies with signed time stamps. Secondly, Integrity guards against alteration of cookies by unauthorized entities by using solutions that can be public-key-based which utilise cryptographic algorithms that sign and digest cookies automatically or be secret-key-based which authenticates cookies against a set of values. Thirdly, confidentiality ensures that values carried by cookies are not exposed to unauthorized entities by being encrypted (2000, pp. 38-41).

3.2 DELIMITATION OF SECURITY METHODS

Although users can be protected by the security methods mentioned by Park and Sandhu (2000), users are still in danger of the vulnerabilities imposed by sites that do not or have not implemented the use of secure cookies, which may still lead to the exposure of personal information on the web. Furthermore, a weak implementation of secure cookies still makes users susceptible to techniques which can bypass the security of cookies, such as the use of replay and volume attacks (Liu, Kovacs, Huang & Gouda, 2005).

4 CONCLUSION

In conclusion, this following review of literature has shown that various researchers have stated or have suggested that there is a need to raise greater awareness in the dangers of the web with respect to exposing personal information on the web, as attackers continually innovate on methods and practices to take personal information from unsuspecting users on the web.

REFERENCES

Consolvo, S., Jung, J., Greenstein, B., Powledge, P., Maganis, G., & Avrahami, D. (2010, September). The Wi-Fi privacy ticker: improving awareness & control of personal information exposure on Wi-Fi. In Proceedings of the 12th ACM international conference on Ubiquitous computing (pp. 321-330). ACM.

Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007, November). A framework for detection and measurement of phishing attacks. In Proceedings of the 2007 ACM workshop on Recurring malcode (pp. 1-8). ACM.

Gross, R., & Acquisti, A. (2005, November). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (pp. 71-80). ACM.

Irani, D., Webb, S., Li, K., & Pu, C. (2011). Modeling unintended personal-information leakage from multiple online social networks. IEEE Internet Computing, 15(3), 13-19.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94-100.

Lam, I. F., Chen, K. T., & Chen, L. J. (2008, November). Involuntary information leakage in social network services. In International Workshop on Security (pp. 167-183). Springer, Berlin, Heidelberg.

Lin, D., & Louiy, M. C. (1998). Taking the Byte Out of Cookies: Privacy, Consent, and the Web.

Liu, A. X., Kovacs, J. M., Huang, C. T., & Gouda, M. G. (2005, October). A secure cookie protocol. In Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on (pp. 333-338). IEEE.

Nohlberg, M. (2008). Securing information assets: understanding, measuring and protecting against social engineering attacks (Doctoral dissertation, Institutionen för data-och systemvetenskap (tills m KTH)).

Park, J. S., & Sandhu, R. (2000). Secure cookies on the Web. IEEE internet computing, 4(4), 36-44.

Ragucci, J. W., & Robila, S. A. (2006, June). Societal aspects of phishing. In Technology and Society, 2006. ISTAS 2006. IEEE International Symposium on (pp. 1-5). IEEE.

Sheng, S., Kumaraguru, P., Acquisti, A., Cranor, L. F., & Hong, J. I. (2009, September). Improving phishing countermeasures: An analysis of expert interviews. In eCrime (pp. 1-15).

Takahashi, H., Yasunaga, K., Mambo, M., Kim, K., & Youm, H. Y. (2013, July). Preventing abuse of cookies stolen by XSS. In 2013 Eighth Asia Joint Conference on Information Security (pp. 85-89). IEEE.

Zheng, X., Jiang, J., Liang, J., Duan, H. X., Chen, S., Wan, T., & Weaver, N. (2015, August). Cookies Lack Integrity: Real-World Implications. In USENIX Security Symposium (pp. 707-721).