Dynamic Passwords for Cross Site Request Forgery

Edinah Ogari, Dr. Abanti, Prof. Waweru, Vincent O.

Institute of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi.

Abstract- Cross-Site Request Forgery (CSRF) is an attack on the privacy of clients of a particular web site which can lead to a total breach of security when the person's details are stolen or manipulated in any way. The CSRF attack involves three parties; the attacker, a client and the web site. The goal of this kind of attack is to steal the client cookies, or any other sensitive information, which can identify the client with the web site. With the token of the legitimate user at hand, the attacker can proceed to act as the user in his interaction with the site. Cross-Site Request Forgery attacks occur when a malicious web site causes a user's web browser to perform an unwanted action on a trusted site. In this way, the attacker can impersonate the user. In this paper, the researcher investigated on the possibility of utilizing dynamic passwords to avert CSRF. The results obtained indicate that 94% of the respondents indicated that the dynamic passwords are 75% perfect in CSRF prevention.

I. Introduction

Cross-Site Request Forgery happens when a malevolent web site causes a user's web browser to perform an unwanted action on a trusted site. Unfortunately, many sites on the Internet fail to protect against CSRF. Since they have been ignored by the web development and security communities, CSRF attacks often exploit the authentication mechanisms of targeted sites (William, 2013). The source of the problem is that web authentication usually assures a site that a request came from a certain user's browser. However, it does not ensure that it is the user who actually requested.

Klein (2009) stated that whenever authentication happens implicitly, as a result of which it is known which site a request is being sent to and which browser it is coming from, there is a danger of CSRF attacks. In principle, this danger could be eliminated by requiring the user to take an explicit, unspoofable action. This may involve re-entering a username and password for each request sent to a site. However, this is bound to cause major usability problems. Cross site request forgery attackers are not required to do extra efforts to carry out attacks because of the way web handles the web application and traffic between client and server which allows them to carry out the attacks. This implies that there are so many flaws which help attackers make their job easy to satisfy their requirement. This is because for an attack to be successful, the user must be logged-in to the target site and must visit the attacker's site or a site over which the attacker has partial control (Rupali, 2012).

II. Methodology

CSRF is an attack which forces an end user to execute unwanted actions on a web application, in which he is currently authenticated. In this section, the researchers gives a series of steps that they followed to achieve their objectives, namely, to use dynamic passwords to avert cross site request forgery.

A dynamic password authentication was proposed by Pansa (2011). In his model, dynamic password was implemented by appending the time string to the password string, before making a single hashing. The user would keep using the same password, until he changes it. Therefore the string to be hashed was the password string + the time. When compared with an original-version of the authentication where only passwords are hashed, it was apparent that the login form would send password string into the password's field together with the time component. This makes the value in the password field to be a variance. This helped the server in verifying the time duration of password creation. In practice, the browser could send the time component via the hidden field. In this model, the time setting of the client and the server must be well-synchronized, by using Network Time Protocol (NTP), or by creating the program on the server in order to postpone the time. The challenge of this mechanism is that if the hacker gets the time component, and the password using mechanisms such as brute forcing and dictionary attacks, then the password can easily be decoded (Elias , 2013).

The solution to the above challenge will be to include more variables to the password field to make it truly variant. In this paper, besides the timing component added before hashing, the network users' username, age, year of birth, and current date were concatenated before hashing was done. This was done to ensure that the generated password is indeed very difficult to guess.

A prototype was designed and developed. It was then availed to the users who interacted with it in real network environment. They gave suggestions for possible improvements which were included in the final system. The researcher then requested the respondents to rate the prototype in terms of its security. The section below outlines the results obtained.

III. Results And Discussion

From the field study, majority (50% and above) of the respondents indicated that the proposed dynamic passwords managed to mitigate the CSRFs in their institutions. This figure was 89% (50%+ 22%+17%). This was done by exposing them to the real usage of the proposed system and allowing them to test it against the known CSRF attack mechanisms (such as HTTP sessions, Image tag, Browsers' view source option and GET and POST methods). Figure 1 below summarizes the obtained results. Therefore, the proposed CSRF mitigation strategy can be regarded as relatively secure and reliable since it is 89% perfect from the research findings obtained.

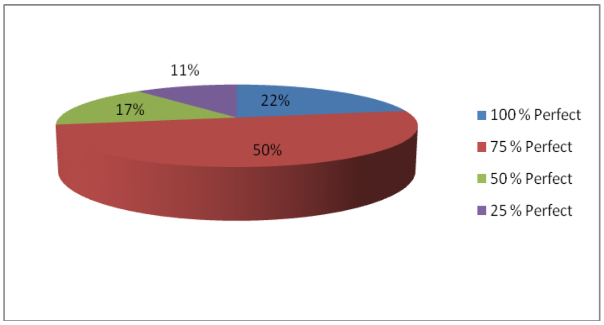

Figure 1: Dynamic Passwords For CSRF

IV. Recommendations

Dynamic passwords have attributes such as unpredictability which makes it difficult for the hacker to guess or crack the password. Also, their constituents are many and varied, hence very difficult for the hackers to determine all of them with great accuracy. The dynamic passwords proposed in this research paper comprise of usernames, static passwords, age, year of birth, current date and current time, all of them concatenated and hashed before the final One Time Password (OTP) can be realized. Due to their dynamic nature, they managed to prevent 75% of the known server attacks. The researcher therefore approves their usage in server –side protection against CSRF.

Other future works in this area may involve the inclusion of biometric identification as one of the constituents of the dynamic generation constituent. This will greatly boost the password's unpredictability as the generated password will involve user-specific details such as DNA analysis.

References

[1] William Z., Edward W., (2013), Cross-Site Request Forgeries: Exploitation and Prevention, Princeton University.

[2] Klein, A., (2009), Cross Site Scripting Explained.

[3] Rupali D., et al, (2012), Computer Network and Information Security CSRF Vulnerabilities and Defensive Techniques, I. J.

[4] Pansa D., et al., (2011), Web Security Improving by using Dynamic Password Authentication, International Conference on Network and Electronics Engineering IPCSIT vol.11 (2011), IACSIT Press, Singapore.

[5] Elias A., (2013), Hunting Cross-Site Scripting Attacks in the Network, Institute of Computer Science Foundation for Research and Technology, Hellas.

Authors

First Author – Edinah Ogari, Institute of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi.
Second Author – Dr. Abanti, Institute of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi.
Third Author – Prof. Waweru, Institute of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi.
Fourth Author – Vincent O. , Institute of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi.