World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:11, No:05, 2017

A Method and System for Secure Authentication Using One Time QR Code

Authors : Divyans Mahansaria

Abstract : User authentication is an important security measure for protecting confidential data and systems. However, the vulnerability while authenticating into a system has significantly increased. Thus, necessary mechanisms must be deployed during the process of authenticating a user to safeguard him/her from the vulnerable attacks. The proposed solution implements a novel authentication mechanism to counter various forms of security breach attacks including phishing, Trojan horse, replay, key logging, Asterisk logging, shoulder surfing, brute force search and others. QR code (Quick Response Code) is a type of matrix barcode or two-dimensional barcode that can be used for storing URLs, text, images and other information. In the proposed solution, during each new authentication request, a QR code is dynamically generated and presented to the user. A piece of generic information is mapped to plurality of elements and stored within the QR code. The mapping of generic information with plurality of elements, randomizes in each new login, and thus the QR code generated for each new authentication request is for one-time use only. In order to authenticate into the system, the user needs to decode the QR code using any QR code decoding software. The QR code decoding software needs to be installed on handheld mobile devices such as smartphones, personal digital assistant (PDA), etc. On decoding the QR code, the user will be presented a mapping between the generic piece of information and plurality of elements using which the user needs to derive cipher secret information corresponding to his/her actual password. Now, in place of the actual password, the user will use this cipher secret information to authenticate into the system. The authentication terminal will receive the cipher secret information and use a validation engine that will decipher the cipher secret information. If the entered secret information is correct, the user will be provided access to the system. Usability study has been carried out on the proposed solution, and the new authentication mechanism was found to be easy to learn and adapt. Mathematical analysis of the time taken to carry out brute force attack on the proposed solution has been carried out. The result of mathematical analysis showed that the solution is almost completely resistant to brute force attack. Today's standard methods for authentication are subject to a wide variety of software, hardware, and human attacks. The proposed scheme can be very useful in controlling the various types of authentication related attacks especially in a networked computer environment where the use of username and password for authentication is common.

Keywords : authentication, QR code, cipher / decipher text, one time password, secret information
Conference Title : ICNSAM 2017 : International Conference on Network Security and Attack Methods
Conference Location : London, United Kingdom
Conference Dates : May 25-26, 2017