RISK ASSESSMENT THROUGH EFFICIENT AUTHENTICATION

[1]S. K. PANDEY & [2]K. MUSTAFA

[1]Department of Information Technology Board of Studies, The Institute of Chartered Accountants of, Noida- 201 309, India

[2]Department of Computer Science Jamia Millia Islamia (Central University), New Delhi-110 025, India

ABSTRACT

Deployed software, now-a-days, are continuously under attack. Attackers have been exploiting vulnerabilities for decades and seem to be increasing their attacks. Firewalls, intrusion detection and antivirus systems cannot simply solve this problem to the desirable extent. Only a concerted effort, by the software development community for building more secure software can foil attackers and allow users to feel protected from exploitation. It is observed that each phase of the SDLC should include the appropriate security assurance mechanism and countermeasures. From requirements through design and implementation to testing and deployment, security measures must be embedded throughout the SDLC phases. Authentication is one of the measure protection mechanisms, which is broadly accepted. Appropriate level of authentication may be well enforce security features and hence ensure security. In this paper, various attributes of 'Authentication' Policy are identified and then a weightage is assigned to each one, followed by the risk assessment to integrate steps for security assurance from the early in the development lifecycle. This will enable the assessment of appropriateness of authentication in terms of risk and lead to counter/additional measures for security assurance.

KEYWORDS: Authentication Policy, Authentication Attributes, Risk assessment for Authentication, Software Security, Security Assurance.