ATTACKABILITY METRICS MODEL FOR SECURE SERVICE ORIENTED SOFTWARE

ABSTRACT

Software based systems are ubiquitous in modern day operations. There has been an increase in software based system attacks; leading to the need to equip the project managers, software designers and software developers with better predictive attackability models at the architectural design stage. Attackability is a concept proposed recently in literature to measure the extent that a software system or service could be the target of a successful attack. The research study aimed to refine the existing predictive metrics models by using the relationship between the internal software attributes: complexity, coupling and cohesion to predict at the architectural design level, an external software attribute, attackability. The model so generated, representing the technical aspect was combined with a social attackability model, to generate a holistic attackability model. The social attackability model is based on identified human traits that make people vulnerable to social engineering attacks. The traits considered are: distraction, social compliance, herd mentality, dishonesty, kindness, time pressure, and need/greed. Mixed methods research was adopted with its pragmatic philosophy. Experimental design was used in the study and to analyze the metrics. Descriptive statistics (frequencies, means and standard deviations) and inferential statistics (Pearson Correlation Coefficients, Kendall tau-b) were used for analyzing experimental data. Results indicate that the six metrics and the refined holistic predictive attackability metrics model are valid. This implies that the metrics can be used as indicators of security threats of service-oriented software systems.