Abstract

Security metrics and measurement is a sub-field of broader information security field. This field is not new but it got very least and sporadic attention as a result of which it is still in its early stages. The measurement and evaluation of security now became a long standing challenge to the research community. Much of the focus remained towards devising and the application of new and updated protection mechanisms. Measurements in general act as a driving force in decision making. As stated by Lord Kelvin “if you cannot measure it then you cannot improve it”. This principle is also applicable to security measurement of information systems. Even if the necessary and required protection mechanisms are in place still the level of security remains unknown, which limits the decision making capabilities to improve the security of a system.

With the increasing reliance on these information systems in general and software systems in particular security measurement has become the most pressing requirement in order to promote and develop the security critical systems in the current networked environment. The resultant indicators of security measurement preferably the quantitative indicators act as a basis for the decision making to enhance the security of overall system.

The information systems are comprised of various components such as people, hardware, data, network and software. With the fast growing reliance on the software systems, the research reported in this thesis aims to provide a framework using mathematical modeling techniques for evaluation of security of the software systems at the architectural and design phase of the system lifecycle and the derived security metrics on a controlled scale from the proposed framework.

The proposed security evaluation framework is independent of the programming language and the platform used in developing the system and also is applicable from small desktop application to large complex distributed software. The validation process of security metrics is the most challenging part of the security metrics field. In this thesis we have conducted the exploratory empirical evaluation on a running system to validate the derived security metrics and the measurement results. To make the task easy we have transformed the proposed security
evaluation into algorithmic form which increased the applicability of the proposed framework without requiring any expert security knowledge.

The motivation of the research is to provide the software development team with a tool to evaluate the level of security of each of the element of the system and the overall system at the early development stages of the system life cycle. In this regard three question “What is to be measured?” “where (in the system life cycle) to measure?” and “how to measure?” have been answered in the thesis.

Since the field of security metrics and measurements is still in the its early stages, the first part of the thesis investigates and analyzes the basic terminologies, taxonomies and major efforts made towards security metrics based on the literature survey.

Answering the second question “Where (in the system life cycle) to measure security”, the second part of the thesis analyzes the secure software development processes (SSDPs) followed and identifies the key stages of the system’s life cycle where the evaluation of security is necessary.

Answering the question 1 and 2, “What is to be measured” and “How to measure”, third part of the thesis presents a security evaluation framework aimed at the software architecture and design phase using mathematical modeling techniques. In the proposed framework, the component based architecture and design (CBAD) using UML 2.0 component modeling techniques has been adopted. Further in part 3 of the thesis present the empirical evaluation of the proposed framework to validate and analyze the applicability and feasibility of the proposed security metrics. Our effort is to get the focus of the software development community to focus on the security evaluation in the software development process in order to take the early decisions regarding the security of the overall system.