AN APPROACH TOWARD SECURITY METRICATION

Abstract

Security has been always a critical issue in industry, IT organizations and academia. One of the most interesting security topics for both researchers and industrial managers is to quantify level of security provided by various security products/tools. This has a critical role in decision making process for CIOs while choosing among different security investments. Therefore there has been large number of approaches suggested for security measurements w.r.t different goals, objectives, and applications. These vary from theoretical and technical to administrative or practical security quantification frameworks.

One of the first attempts in security metrication has been to find a single overall metric of security. However as security is a multi-faceted property, there have been practical/fundamental problems to achieve such a metric. Moreover most of the security metrication approaches are basically design and development metrication and thus not applicable in evaluating operational security. Therefore, we suggest a framework for security metrics that is based on a number of system attributes (dependability and security), and the system's interaction with the environment via its boundaries. We propose metrication methods based on an existing model integrating the traditional CIA aspects of security with dependability attributes. By taking the black box approach, we suggest that there should be metrics related to protective attributes, to behavioural attributes and to system correctness. Moreover we discuss the relation between these types of metrics and the cause-effect concept. We are convinced that this approach will facilitate developing practical and operational security metrics that refer to attributes that are well-defined, as opposed to most existing metrics, which refer to a security concept that is not well-defined.

PhD student: Laleh Pirzadeh

Supervisor: Erland Jonsson

Chalmers University of Technology