Chapter 2
Quantitative Security Assurance

Basel Katt
Norwegian University of Science and Technology, Norway

Nishu Prasher
Statistics Norway, Norway

ABSTRACT

Security assurance is the confidence that a system meets its security requirements and is resilient against security vulnerabilities and failures. Existing approaches can be characterized as (1) qualitative in nature, (2) tend to achieve their goals manually to a large extent, (3) very costly, (4) development-process oriented, and finally, (3) treat all security requirements within one domain equally for all applications regardless of the context. In this chapter, the authors propose a security assurance framework and its assurance evaluation process. The framework and process depend on a quantitative security assurance metrics that were developed too. The proposed metric considers both the security requirements and vulnerability. Weight has been introduced to the security requirement metric to measure the importance of security requirements that need to be fulfilled. The framework with the proposed quantitative assurance metrics are evaluated and validated using two field case studies related to two operational REST APIs that belong to and are used by Statistics Norway.

DOI: 10.4018/978-1-5225-6313-6.ch002

INTRODUCTION AND BACKGROUND

Assurance can be defined as the estimate of the likelihood that a system will not fail in some particular way (Anderson, 2010). Consequently, security assurance can be defined as the estimate that the system will not be compromised in some particular way. According to the National Institute of Standard and Technology (NIST) (Kissel., 2013), assurance is defined as following as the *"Grounds for confidence that the other four security goals (integrity, availability, confidentiality and accountability) have been adequately met by a specific implementation.* "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or bypass.". According to (Ouedraogo, Mouratidis, Khadraoui, Dubois, & Palmer-Brown, 2009) security assurance is defined as the confidence that the system meets its security requirements. Further, authors in (Spears, Barki, & Barton, 2013) define security assurance as the degree of confidence that security needs are satisfied, and it represents the level of trust we give to the system (Bischop, 2002).

We define *security assurance* as the confidence that a system meets its security requirements and is resilient against security vulnerabilities and failures. The confidence indicated by the security assurance represents the level of trust we give to a system that is safe to use. W*e assume that an assurance scheme (will be defined later) contains the set of goals and objectives that need to be achieved to reach a particular level of assurance. Such goals can be defined in terms of requirements that need to be fulfilled, or vulnerabilities and threats that need to be avoided.* Evaluation, on the other hand, can be defined as (Anderson, 2010) (Bischop, 2002) "*the process of gathering and analyzing evidence that a system meets, or fails to meet, a prescribed assurance target". Assurance technique* (Such, Gouglidis, Knowles, Misra, & Rashid, 2016), *or activity, is defined as a method of assessing an assurance target.*

This means that *evaluation* represents the process of evidence assembly and level assessment, while an *assurance technique,* represents the technical method that is used in the evaluation process for assessment. Assurance scheme in some standards, like *the Common Criteria (CC)*[1], *can be defined in terms of security requirements and assurance requirements.*

Evidence collected in the evaluation process will be defined in terms of measurements associated with a set of defined security metrics. A security metrics can be defined as a measure that depicts the security level, security performance or security strength of a system [5]. Authors in [35] categorize security metrics based on four key dimensions (1) metrics of system vulnerabilities (2) metrics of system defense strength (3) metrics of attack (or threat) severity (4) metrics of system dimension or situations. In the context of security assurance, we define a security