CHAPTER 2

Security Metrics Background & Preliminaries
2. SECURITY METRICS BACKGROUND & PRELIMINARIES

2.1 Introduction

With a shift from standalone application to the complex interconnection of insecure components and networks, the information systems especially the software systems are becoming more and more vulnerable. Verities of protection mechanisms and security approaches are applied but the resulting security level remains unknown. Like other software quality attributes, the level of security a system possess need to be outlined and measured. Such security metrics can be utilized in many ways to benefit an organization, including increasing accountability, improving security effectiveness, and demonstrating compliance [Alger et al., 2001] “How much secure a software system is? “ “How secure does a system need to be?” “What are the factors responsible for the security of the system?” and “The stages in the software development where the security need to be evaluated”, these are questions that are asked to those who work to evaluate the efficiency of security efforts. The answer to all these questions can be only possible if we have such security metrics that evaluate the system for security and provide the evidence of the security level and performance of the System under investigation.

In particular to the software systems several quality attributes, such as reliability, size, complexity etc. have been investigated and evaluated. Very least attention has been remained towards the evaluation of security. Literature surveys showed that the security is an emerging concern in the current times ranging, from an organization to an individual. The area of security metrics is very hot and demanding but at the same time the field is very young [Jansen, 2010]. The problem behind the immaturity of security metrics is that the current practice of information security is still a highly diverse field and holistic and widely accepted approaches are still missing [Savola, A 2007]. The field still aims mainly at the basic definitional aspect and lacks in well-structured literature at hand. According to [Savola A, 2007] in order to make an advance in the field of measuring, assessing or assuring security, the current state of the art should be investigated thoroughly. In this chapter we present the preliminaries of the field of security metrics and based on the literature survey analyze the relevant major effort made for measuring the security of information system in general and for the software system in particular.

The rest of the chapter is organized as: Section 2.1 presents some preliminary concepts of security metrics, theirs properties and objectives. In section 2.3 investigates and presents some major taxonomies in the field of security metrics, Section 2. 4 presents some of the major efforts made
towards the actual measurement in a classified manner, followed by the section 2.5, which presents the conclusion

2.2 Security Metrics Concepts

To understand security metrics, we must first differentiate between the metrics and measurement. Measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline two or more measurements taken over time [Jelen, 2000]. Measurements are generated by counting; metrics are generated from analysis [Alger, et al., 2001]. In other words, measurements are objective raw data and metrics are either objective or subjective human interpretations of those data. The well-developed security evaluation framework and derived metrics can act as an effective tool for security manager to discern the effectiveness of various components of their security programs, a system, a product or process [Payne, 2006]. Such security metrics certainly enables the development team to provide the necessary protection mechanism to ensure the secure system development. As mentioned earlier security metrics have many interpretations. Below are some of short elaborations of term security metrics.

- According to [SSE-CMM, 2011], metrics are quantifiable measurements of certain aspects of the system or enterprise. Such measurement is based on some attributes of the system that are responsible for the security of the system. Further, a security metric is a quantitative measure of how much these attributes the system possess.

- According to [Swanson. M et al., 2003], metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data such that the end results aim to facilitate in taking the required corrective measures.

- According to [Payne, 2006] measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline two or more measurements taken over time. Measurements are generated by counting; metrics are generated from analysis. In other words, measurements are objective raw data and metrics are either objective or subjective human interpretations of those data.
In their work [Farooq et al., 2011], outlined the importance of measurements and metrics and their relation to the software testing. In the same work [Farooq et al., 2011] analyzed the process of software measurement process in general, which is comprised of following key stages.

- **Planning**: Defining the procedure and scope of the measurement process.
- **Implementation**: The actual application of measurement process and procedure defined at the planning stage. The output of this stage should be in the form reports of performance related data.
- **Improving**: Based on the process and progress evaluation (through the reports generated in the implementation phase) the necessary decision is to be taken in order to make an improvement to the system.

The output scale of the software measurement and metrics is possibly hierarchal in nature, which is comprised of various levels. Each level scale in the hierarchy possesses all the properties of lower level scale in the hierarchy. In the same work [Farooq et al., 2011] identified the five measurement scale based on the literature survey.

### 2.2.1 Characteristics of Security Metrics

According to [Jelen. G, 2000], security metrics should be SMART, i.e. Specific, Measureable, Attainable, Repeatable, and Time dependent. Security metrics should be able to identify and measure the degree of security attributes like confidentiality, integrity and availability of a system. The method of measurement employed should be reproducible, that is, capable of attaining the same results when performed independently by different evaluators [Jansen, 2010]. The ultimate goal of security metrics should be to mitigate the security risk and act as a tool for decision making especially in *assessment* or *prediction*, for the development team and other stockholders. When the target is to predict the security level of a system then mathematical model and algorithms are applied to the collection of measured data (e.g. regression analysis) to predict the security of the system, process, or product. Our security metric framework is based on the *prediction* method where mathematical modeling techniques has been adopted and finally the security evaluation process is transformed into an algorithmic form. It is important to clearly know the entity that is the target of measurement because otherwise the actual metrics might not be meaningful [Savola, 2008]. Federal Information Processing Standards [FIPS, 2004] provides a mechanism for the investigation of confidentiality, integrity and availability separately. As the
security requirements for each of the system or organization vary according to the needs, so the security evaluation should be based on the well-defined security attributes such as confidentiality, integrity, availability, privacy, nonrepudiation etc.

### 2.2.2 Security Metrics: Properties

Security metrics properties can be investigated based on the following classification [Savola, A 2007]

- **Quantitative vs. Qualitative metrics**: The end result of the security metrics may be either quantitative or qualitative in nature. The quantitative results are preferred over the qualitative one because of the discrete measurable nature of the results. At the same time the generating the quantitative metrics are more challenging than the quantitative one.

- **Objectivity vs. Subjectivity of Security Metrics**: As with the case of quantitative vs. quantitative the resultant security metrics should be either objective or subjective in nature. Objective security metrics is the preferred one and portrays the security posture of a system or process in certain discrete levels such as low, medium, and high on a scale. The subjective metrics normally takes into consideration the human behavioral aspects in the security.

- **Direct vs. Indirect metrics**: Direct metrics are those that measure an atomic attribute of the system in a sense that the measured attribute responsible for the security does not depend on the other attributes, whereas indirect metrics involve multiple attributes that are interdependent.

- **Static vs. Dynamic metrics**: Result of the dynamic metrics will be effected by the time elapsed whereas static metrics do not take the time into the account.

- **Absolute vs. Relative metrics**: An absolute metrics is atomic in nature in a sense that it does not depend on the output of any other metric, whereas relative one does.

### 2.2.3 Security Metrics Objectives:

The main objective of the security metrics is to gauge into the system for the level of security it possess, such that the most critical elements of the system with respect to the security can be identified. According to [Savola, 2009] security correctness, security effectiveness and security efficiency are main three objectives of the security measurement, defined as:
– **Security Correctness**: ensures that security enforcing mechanisms have been implemented correctly in the system under investigation and system meets its security requirements.

– **Security effectiveness**: ensures that stated security requirements are met in the system under investigation and the system does not behave in any way other than what it is intended.

– **Security efficiency**: ensures that the adequate security quality has been achieved in the system under investigation.

### 2.3 Security Metrics taxonomies

Since the area of security metrics is still in its early stages with varying definitions and terminologies. Various security metrics taxonomies exists in the literature that aim at the categorization of security metrics at higher level of abstraction. Based on the literature survey in this section we look at some of the most common among them.

In [Swanson, 2001], [Swanson et al., 2003], NIST presented a security metrics taxonomy, which categorized the security metrics into three modes i.e. Management, Technical and Operational. It further presents 17 sub categories of metrics each with examples. The focus of this taxonomy is from the organizational and stockholders perspective, rather than the technical perspective of a particular system. Below diagram 2.1 depicts the classification of security metrics proposed by NIST.

In their study [Henning et al, 2002], workshop on Information Security System, Scoring and Ranking (WISSR) provides a detailed discussion on issues related to Information Assurance (IA). They used the term IS* for Information Security. The (*) with IS is related to security measurement and can be used to denote the terms like metric, scores, ratings, rank, assessment results etc. The work shop did not propose any new specific security metric taxonomy, instead it was organized into three tracks; technical, operational and organizational based on the interest of the participants. Technical metrics are used to describe and compare the technical objects such as an algorithm, specification, design etc. Operational metrics are used to manage the risk to the operational environment and the organizational metrics are used to describe and track the effectiveness of organizational program and process.
In their study [Vaughn et al., 2003] proposed a taxonomy for Information Assurance (IA) metrics. They divided the taxonomy into two distinct categories of security metrics (a) *Organizational security metric* (b) *Technical Target of Assessment* (TTOA). The former aims at providing the feedback to improve the security assurance status of the organization. The second category metrics (TTOA) is intended to measure the security capability of a particular system or product. Both categories are further categorized in order to put the specificity in terms of measuring security. Above figure (2.2) shows the higher level classification of the taxonomy.
In their [Seddigh et al., 2004] proposed a new taxonomy for IA (information assurance) and IT networks that aim to provide the basis and motivation for the research in overcoming the challenges in the area. In Their taxonomy the metric space is divided into three categories: Security, QoS, and Availability. Each of these categories is further categorized into three subcategories as technical, organizational and operational metrics, which are further categorized into 27 classes. According to them, organizational metrics evaluate an IT organization’s emphasis on IA (Information Assurance) in terms of goals and organizational policies. Technical metrics evaluate the technical components of an IA network and also the subset metrics under this category provides the rating, incident statistics and security testing. Operational metrics evaluate the operations of an IT organization in terms of complying with the goals and policies.
set by the organization. Figure (2.3) shows the proposed taxonomy by the authors at the higher abstract level of classification.

In his study [Savola. A, 2007] proposed a security metrics taxonomy based on the literature survey. The main aim of the author is to bridge the gap between Information Security Management and Information and Communication Technology Industry (ICT). In this taxonomy the author’s intent was to enhance the composition of feasible security metrics all the way from the business management to the lowest level of technical details. This taxonomy categorized the security metrics in a tree like structure into six levels from L0 to L5 with business level security metrics at the root (L0) and the implementation level technical metrics at the leaf nodes (L5). At the higher level, business level security metrics are divided into five sub categories, (i) Security metrics for cost-benefit analysis, containing economic measures such as ROI (return on investment) (ii) Trust metrics for business collaboration (iii) Security metrics for information security management (ISM) (iv) Security metrics for business level risk analysis (v) Security
dependability and trust (SDT) metrics for ICT product system and service. The author further provided the sub categories of the above category (iii) and (v). Below diagram shows the classification of security metrics taxonomy.

All the proposed security metrics taxonomies are conceptual and abstract in nature. Very little has been reported on the actual scale of measurement. From these taxonomies it is evident that a great deal of efforts is needed to devise the metrics that can be applicable in real practices.

2.4 Software Security vs. Software Reliability Measurement: An Overview

Software reliability always remained an important quality attribute of the software system and various efforts to evaluate and measure the reliability has been made. The idea of security and reliability are technically derived from the requirement to describe correctness. Both the terms have grown up in different domains of thinking. Security can be defined as a functional statistical predictability statement where the answer to the question being secure or not is whether a given system specified can be expected to continue to function for some period in some specified manner. Reliability can be defined as a functional statistical predictive statement of predictability where a system in reliable state or not is whether a given system can be expected to continue function for some specified period in some specified manner [Roy D. Follendore, 2002].

Reliability and security are not the isolated from one another; instead reliability has a great impact on the security of a system. The "reliability of security" is often considered but the "security of reliability" is not often considered [Roy D. Follendore, 2002]. As far as software measurement is concerned the various efforts have been made to device the new and updated
metrics, models and measurements techniques to evaluate the reliability of the software systems and very least efforts to evaluate the security of software system has been made. The main problem behind it may be the multifaceted nature of security and the dependency of security on the various other qualities attributes like testing and reliability of the software systems. In their work [Farooq et al., 2012], presented an in depth analysis of the key concept, metrics, models and measurement used in software reliability. Since the reliability is the probability of a system or components to perform its required service without failure under stated conditions for a specified period of time [Farooq et al., 2012]. Various probabilistic models and methods have been proposed to predict the reliability of a system. Among the proposed model and methods the software reliability growth models (SRGM) has been used to predict the reliability of the systems. SRGM shows how reliability of a system improves in a period of time when the faults are detected and repaired. SRGM is actually used to determine when to stop testing to attain a given reliability level [Quadri S. M. K et al, 2011]. Over the last three decades many efforts have been made to develop the SRGMs. Among them [Musa et al., 1887], [Xie, 1991], [Lyu, 1996], are the most common SRGMs and verities of metrics like number of remaining faults, mean time between failure (MTBF), and mean time to failure (MTTR) have been derived. In the later times [Bokhari and Ahmad, 2006], [Quadri S.M. K et al, 2006] proposed the probabilistic software reliability growth model based on Non-homogeneous Poisson process (NHPP) which incorporates the testing efforts. Further in their work [Quadri S.M.K et al, 2011] a scheme for constructing software reliability growth model (SRGM based on (NHPP) have been proposed.

Table 2.1 Software Reliability Prediction Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Year</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ohba exponential model</td>
<td>1984</td>
<td>[Ohba, M. 1984]</td>
</tr>
<tr>
<td>Yamada Rayleigh model with Weibull curve</td>
<td>1993</td>
<td>[Yamada , S et al , 1993]</td>
</tr>
<tr>
<td>Quadri’s NHPP SRGM with generalized</td>
<td>2006</td>
<td>[Quadri S.M.K et al, 2006]</td>
</tr>
<tr>
<td>exponential testing efforts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quadri’s SRGM based on (NHPP)</td>
<td>2011</td>
<td>[Quadri S.M.K et al, 2011]</td>
</tr>
</tbody>
</table>
Above table (2.1) summarizes the major efforts made towards modeling the reliability prediction of software system based on the software reliability growth models (SRGMs). On the other hand there exists no such probabilistic model to predict the security level of the system over a specified time period. Systematic efforts are needed develop the models and methods to predict the security of the software systems. The methods and models of reliability prediction can used to understand the state of art of prediction and measurement.

### 2.5 Related Work

Security metrics can be obtained at different levels within an organization or a technical system. Detailed metrics can be aggregated and rolled up to progressively higher levels. The various efforts made on actual metrics development are sporadic in nature, some taking into the consideration the knowledge of previous and current vulnerabilities; some measure the code quality some strike at the design of a system. From the literature survey, at the higher level these efforts can be categorized as following based on the major factors taken into the consideration in measuring the security of a system as:

- **Analyzing the capabilities of attacker**: Under this the security of a system is measured by taking into account the required efforts, capabilities and resources of an attacker.

- **Knowledge of Vulnerabilities**: Under this category the security evaluation is carried out by taking into account the knowledge of both the vulnerabilities reported in past and present vulnerabilities.

- **Conceptual**: Under this category the security metrics are based on the knowledge of the personnel regarding security and are conceptual in nature, having very limited use in real practices.

- **Independent**: Such security metrics are based on the analysis of the attributes of the system itself (inner attributes) and are predictive in nature. Security metrics under this category are highly desirable to ship the more secure and less vulnerable systems.

Our proposed security metrics framework in chapter (4) comes under forth category i.e. it is independent of the external security factors and is based on the internal attributes of the system.

In their study [Manadhata et.al, 2007] proposed the system attack surface as an indicator to the security of a system and formalized the system attack surface using I/O automata model. The attack surface of a system is comprised of three kinds of resources that an attacker can use to...
carry out an attack on the system. These resources are the methods, channels and data of the system. Based on the direction of flow of data they further technically defined the entry points and exit points of the system which are actually the methods of system through which the flow of data takes places. Authors defined the attack surface as subset of system resources that an attacker can utilize carrying out attack on the system and accordingly quantifying the resultant security indicators. Larger the attack surface of a system more the system vulnerable to the attacks. Further the authors analyzed the feasibility of the proposed approach by measuring the attack surface of open source FTP daemons and two IMAP servers.

Major efforts made towards the security measurement by taking the capabilities and resources of an attacker into consideration also known as attacker-centric security metrics are [Leversage et al., 2008], [Miles et al., 2005] and [Ortalo et al., 1999]. In these studies the security measurement is carried out by analyzing the ways an attacker can carry out the successful attack on the system with respect to the knowledge and resources at hand. In contrast the proposed security metric framework in this thesis chapter (4) is based on the system architecture and design. Being an independent of attacker’s capabilities our proposed framework act as a tool for the software development team to measure the inherent security of the system and enables them to take the necessary decisions regarding security.

[Littlewood et al., 1993] proposed a conceptual model based on probabilistic methods which initially used for reliability analysis, to measure security of a system. In their conceptual model they proposed the usage of the efforts made by an attacker to carry out a successful attack on the system as a measure of system’s security.

In the second category where the knowledge of vulnerabilities reported in past and the present vulnerabilities [Alhazmi et al., 2006] proposed a vulnerability density (VD) metric which is defined as the number of vulnerabilities in a unit size of code. From the VD the authors further proposed a set of metrics such as vulnerability discovery rate (VRD) which is the number of vulnerabilities identified per unit time and known vulnerabilities density (VKD). In contrast the proposed security metric framework in this thesis chapter (4) is independent of the knowledge of the past or present vulnerabilities.

[Alves-Foss et al., 1995] proposed the measurement of a system using System Vulnerability Index (SVI) as a measure of system vulnerability to common intrusion methods. SVI is
2. SECURITY METRICS BACKGROUND & PRELIMINARIES

calculated by evaluation the various factors like “system characteristics”, “potentially neglectful acts” and “potentially malevolent acts”.

[Voas et al., 1996] proposed the security metric based on the technique of deliberate fault injection. The fault injection is carried out by simulating the threat classes of the system by mutating the variables during the execution and then observing the impact of threat class on the behavior of the system. Finally they have proposed a minimum-time-to-intrusion (MTTI) metric based on the time before any simulated intrusion can take place.

[Schneier, 1999] proposed the attack tree to analyze the security of a system. The attack tree is constructed by setting the attackers goal as the root and branches of the tree as the different ways that an attacker can adopt to carry out the attack on the system along with the cost involved along with each of the possible path to carrying out the attack. The cost estimation becomes the measure of the system security. The prerequisite to generate an attack tree is the knowledge about attacker’s goals, system vulnerabilities, and attacker’s behavior.

Many other conceptual security measurement efforts are made by [Littlewood et al, 1993], [Madan et al., 2002],[Stuart, 2004]. These metrics are conceptual in nature and haven’t been applied in real security evaluation of the systems.

2.6 Conclusion and Future Scope

In this chapter we have analyzed the preliminaries and various concepts of the security metric field. From the presented taxonomies of the security metrics, it is evident that the field of security evaluation is multifaceted and wide open challenge for the organizations and research community. In practice very little has been delivered on the actual scale and it needs a systematic approach to make the progress in this area. Based on the literature survey we have classified the efforts made in the field of security metrics and presented the major efforts made towards the security metrics of the software systems