Advanced Security Metric Model : ASM

Manju Khari , Divya Nigam
Department of Computer Science and Engineering, AIACTR, Delhi , India

Abstract: Security metrics is an area in computer security that has been receiving adequate attention. Majority of works done in the domain of security metrics is mainly definitional, targeted towards providing guidelines for defining a security metric and specifying criteria for which to strive to achieve security. As far as security metrics models are concerned, only a few models have offered the quantitative basis for giving security assurance. Advanced Security Metrics model is a seven layered model in which every layer deals with a specified category of metrics related to specific categorization. This model deals with following parameters namely Initial vulnerability parameter, Repeated vulnerability parameter, Remediation latency parameter, Sensitive information vulnerability parameter, Exceptional handling Parameter, Unexpected vulnerability parameter, Network Vulnerability Identification Parameter at different levels and Network Vulnerability Parameter. The Value of every parameter decides the level of security the application is having.

Keywords: Security Metrics, Risk Analysis, metrics

1. Introduction

Metrics are considered as measures which are used for measurement, comparison or to track performances. As far as software metrics are concerned, they help us to make meaningful estimates for software products and help in taking managerial and technical decisions. The coverage of the security metrics is broad and it ranges from mathematical consideration for measuring technical security elements such as Antivirus effectivity and application security to managing security programs[13]. Security metrics is an adequate area in computer security. It has been receiving adequate attention in recent times. Majority of works which has been done in this field is actually definitional. It has targeted towards providing the guidelines for defining a security metric. A very little work has only been done in this field and some part of it has brought in practice. There is always the confusion about the distinction between measurements and metrics. Not only this their interpretation as well as their validation are also very confusing. Measurements are generally possible and inform us about the quantitative characteristic of a software, network or system like extent, dimension, capacity, size, amount etc. But measures are normally useless if adequate interpretations of it are not available except in the case of direct comparison with other measures. As far as information security metrics are concerned, they are important factor in making valuable decisions about various regions of security. They actually range from the design of security architectures and controls to the effectiveness and efficiency of security operations. The coverage of the security metrics is broad and it ranges from mathematical consideration for measuring technical security elements such as Antivirus effectivity and
application security to managing security programs[12].Jaguith who is called the guru of security metrics suggested that metrics should measured and expressed as the percentage or the cardinal number not as labels like High, Low and medium. There should be one unit of measurement for that metrics for example defects etc. Jaguith expressed mathematical arithmetic is not complete mathematical way to calculate overall security risk scores. Examples are high = 3, Medium = 2, Low = 1, These are not correct way to calculate risk or measure security metrics. Most of the security metrics being developed usually measures technologies being used, technical process if effective or not and inputs etc but there is a more need to take into consideration management processes and results or outcomes of information security.

There is a recommendation to select initial metrics for implementation which have certain qualities and then after there is a need to score as well as weight them.

I. Mathematical representation of security metrics

\[ SM = \sum_{i=0}^{n} WiXi \]

Where \( SM \) = Security Metrics, \( n \) = Number of parameters, \( W \) = Weight value or impact value, \( X \) = Measurable potential weak spots for a parameter

The basic difference lies in the fact in which scenario the metrics is working. Based on the project what may differ is, the parameters of security, the weighted values and the method of calculating it. Whatever the case may be but the end result is that security metrics is nothing but the weighted sum of the number of potential weak spots identified within a project. An attempt has been made to map equation (ii) to the security of a web page which is a common platform for modern business transactions.

2. Past Security Metrics Model

- **Information security measurement model (ISO27004)**

These key terms deals with ISO 27004 model. They are as follow:

- **Analytical Model:** It can be called as Algorithm or calculation which combines one or many base as well as derived measures which are associated with decision criteria. It based on relative understanding, assumptions and the expected relationship between the base measures as well as the derived measure and their behaviour over time. An analytical model signifies the estimates relevant to the defined as well as corresponding information.

- **Indicator:** It is a measure that provides an estimate or evaluation of specified attributes which are derived from an analytical model with respect to a defined information need. Indicators are the basis for analysis as well as decision making.

- **Decision Criteria:** Basically decision criteria depends upon the Thresholds, targets, or patterns and these are used to determine the need for action, or they help to describe the level of confidence in a given result and its interpretation.

- **Object:** They are basically the things that is characterised through the measurement of its attributes. An object may include processes, plans, projects, resources, and systems.

- **Measurement Method:** It's a sequence of operations used in quantifying an attribute with respect to a specified scale.
- **Base Measures**: It is a measure which is defined in terms of an attribute and the specified measurement method for quantifying it (e.g., number of trained personnel, number of sites, cumulative cost, etc). After the data collection, a value is assigned to a base measure and that is basically measured in terms of parameter.

- **Derived Measures**: A measure which can be derived as a function of two or more base measures is called derived measures.

- **Katzke’s Model (2001)**
  The metrics of this model are consist of object need to be measured, the objectives of security and measurement method. The key features of this model are:
  
  - **Measurement method** can be direct testing, evaluation procedure, training procedure and observation of performance of system.
  - **The objects which need to be measured** can be anything like an organization or product or a process.
  - **The security objective** being set against which the measurement have been taken can be security requirements, best practice standard, security baseline or maturity capability of the models.

- **Deborah Bodeau’s Model**
  In this model, metrics were defined as the cross product of target to be measured, why to measure it and the audience. The following key features of the model are identified:
  - **Target to be measured** can be technical, process, organization or system.
  - **The purpose of measurement** may be for complete description as well as comparison or for prediction.
  - **The intended audience** for which target is being measured includes technical experts, decision and policy makers.
• QUANTITATIVE METRICS AND RISK ASSESSMENT MODEL

Features of this models are as follow:

- **System Susceptibility**: system confidentiality, integrity, and availability cannot be maintained and achieved collectively. If somehow attacker access and test the system before actual attack. This access can provide great opportunity.

- **Threat Accessibility**: In this phase, accessible susceptibility are

identified. It’s a superset of legitimate user access as some access points are not authorised.

- **Threat Capability**: In this phase capability of attacker to steal the information is being analysed.

- **Peter Mill’s Model (2009)**

  This model categorized metrics on the basis of base metric group, temporal metric group and environmental metric group in order to measure overall vulnerability score.

  The major features of this model are:

  - The Base metric group consists of access complexities related to access, authentication, confidential as well as integrity bias and impact bias.
  - Temporal group consists of level of exploitability with time factor and remediation level.
  - Environmental group is formed so formed depends upon potential level of collateral damage as well as target distribution.
• Reijo M. Savola’s model (2009)

In this context, metrics has been modelled in quite twisted form showing many important and vital points of the system being measured. The levels of this model are summarized as below:

- Level 0: In this level, Target system is being investigated.

- Level 1: In this level, Main view points of the target system are categorised. They include level of security quality of targeted system, level of security enforcing controls, and security level of system life cycle, project and business management.

- Level 2: Elementary objectives of measurement are being identified. The purpose of this level ensures the level of correctness as well as efficiency of the system as well as effectiveness of the system.

- Level 3: This level deals with those components which are measurable. Hence, the measurable components are identified in this level. They include the requirements and the design specifications.

- Level 4: This level deals with detailed metrics features. This level gives the detailed information about the selected components of the system which is put under the investigation.

• Steve Christey’s model (2011)

The metrics considered under this model are called as Common Weakness Scoring system which is a summation of base finding group, attack surface group and exploitability group. These groups are explained as below:

- Base finding group score is calculated from impact bias, finding confidence, remediation cost, and prevalence.

- Attack surface group score is calculated from access vector, universality, Strength of authentication, required privilege level requirement, and instance of authentication.

- Exploitability group. The score for this group depends upon the likelihood of exploitability, discovery, level of interaction, effectiveness of internal and external control.

ASM MODEL (Advanced Security Metrics model)

The proposed web application security model named as Advanced security Model. In this model we have specified seven key areas which need to be
measured to ensure of getting a web security program. It is to be kept in mind that before going depth into the metrics, the goal should be fully specified that what are the goals.

1. **Total initial vulnerabilities**: These are the vulnerabilities which are being identified by scanner but can also be identified by manual analysis. Firstly, this need to be measured and can be called as Initial vulnerability parameter.

   \[
   IVP = \frac{ACTUAL\ INITIAL\ VULNERABILITY}{ESTIMATED\ INITIAL\ VULNERABILITY}
   \]

2. **Repeated vulnerabilities**: Those errors or flaws which keep appearing again and again with the reason of not being resolved. This parameter is called as Repeated vulnerability parameter.

   \[
   RVP = \frac{ACTUAL\ REPEATED\ VULNERABILITY}{ESTIMATED\ REPEATED\ VULNERABILITY}
   \]

3. **Latency related to remediation**: It deals with the time taken by the window to deploy the fix and with many other details such as severity rating. It also deals with specific problem such as coding or server configuration. This parameter is known as Remediation latency parameter.

   \[
   RLP = \frac{ACTUAL\ TIME\ TAKEN}{ESTIMATED\ TIME}
   \]

4. **Vulnerabilities which are exploitable by placing sensitive information at lots of risk**: It includes SQL injection, XSS. This parameter is called as Sensitive information vulnerability parameter.

   \[
   SIVP = \frac{ACTUAL\ RISK}{ESTIMATED\ RISK}
   \]

5. **Vulnerabilities that do not lead to immediate danger**: It includes ASP.NET debugging being enabled, unhandled exceptions, IP addresses being revealed, etc. This parameter is known as Exceptional handling Parameter.

   \[
   EXP = \frac{ACTUAL\ UNHANDLED\ EXCEPTIONS\ PRERELEASE}{ESTIMATED\ U\ EXCEPTIONS\ (PRERELEASE+POSTRELEASE)}
   \]

6. **Unexpected vulnerabilities that are not present but can be sought out on the systems based on data and information in our server and application logs**: This parameter is known as Unexpected vulnerability parameter.

   \[
   UVP = \frac{ACTUAL\ UNEXPECTED\ VULNERABILITY\ PRERELEASE}{TOTAL\ (U\ V)\ PRE\ RELEASED + POST\ RELEASED}
   \]

7. **Vulnerabilities being identified by network traffic analysis**: It includes password cracking, denial of service attacks such as the slow HTTP attack, etc. This parameter is known as Network Vulnerability Identification Parameter at different levels.

   \[
   NVIP = \frac{ACTUAL\ LEVEL\ OF\ NETWORK\ VULNERABILITY}{ESTIMATED\ LEVEL\ OF\ NETWORK\ VULNERABILITY}
   \]

Overall vulnerability score can only be measured by measuring all the individual vulnerability levels and identifying the over all score on the basis of it.
Figure 5: Respected Parameter measured by Asm Model

Figure 6: Vulnerability to be measured
References


Authors Bibliography;

Manju Khari (manjukhari@yahoo.co.in) is a research scholar with Delhi Technological University (formerly Delhi College of Engineering), Delhi, India. She is an Assistant Professor in Ambedkar Institute of Advanced Communication Technology and Research, Guru Gobind Singh Indraprastha University, Delhi, India. She received her Masters degree in Information Security from Ambedkar Institute Technology, Guru Gobind Singh Indraprastha University, Delhi, India. Her research interests are software testing, software quality, software metrics and optimization algorithm. She has published several papers in international journals and conferences.

Divya Nigam (divyanigam90@gmail.com) is pursuing M.tech in Information Security from Ambedkar Institute of Advance Research and Communication, Guru Gobind Singh Indraprastha University, Delhi, India. She has completed her B.Tech in Information technology from Guru Prem Sukh Memorial college of Engineering, Guru Gobind Singh Indraprastha University, Delhi, India. Her research interests are software security testing.