CHALMERS
UNIVERSITY OF TECHNOLOGY

Chalmers University of Technology

Methodologies and Approaches to Measure Security

Master's thesis in Computer Systems and Networks

FAUSTINE NYANGIRA

MARVIN T. NGOMA

Department of CSE
GOTHENBURG UNIVERSITY | CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2016

Master's thesis 2016:

Version 1.6
Date: 2016/10/27

Methodologies and Approaches to Measure Security

FAUSTINE NYANGIRA
AND
MARVIN T.NGOMA

Department of Computer Science and Engineering
Gothenburg | Chalmers University of Technology
Gothenburg, Sweden 2016

Methodologies and Approaches to Measure Security

FAUSTINE NYANGIRA

AND

MARVIN T.NGOMA

Supervisor: Erland Jonsson, Chalmers University of Technology
Examiner: Riccardo Scandariato, Department of Software Engineering
Master’s Thesis 2016:
Department of Computer Science and Engineering
Gothenburg Chalmers University of Technology
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Cover: To measure is to know!

Printed by [Chalmers library]
Gothenburg, Sweden 2016

ABSTRACT

Security has today become a topic of cardinal interest in many companies and organisations. To deal with security and its management, it is a good idea to be able to quantify it in order to know how secure a given system is, i.e. to metricate security.

Many approaches to security metrication have been suggested, but most of them rely upon experts' subjective judgement rather than being based on objective measures or scientifically sound methodology. Further, there is a large diversity in the existing metrication methods with respect to approach, objectives, goals and result. This calls for a systematisation and structuring of the field in order to get better knowledge of the benefits and usage of different metrication methods.

The goal of this work is to study the methodologies and approaches towards metrication activities as suggested by various stakeholders. Specifically, we will look at how each approach develops, selects and implements information level measures for the purpose of showing the effectiveness and efficiency of the security objectives and their related activities. We will then analyse how these measures can be used by an organization for the identification of the adequacy of its implemented processes, policies and procedures. Nevertheless, we will propose a systematized model for measuring security and devising security metrics.

Keywords: *confidentiality, Integrity, availability, Reliability, safety, maintainability.*

Acknowledgements

We would like to sincerely say thank you to our supervisor, Prof. Erland Jonsson, who has been of great guidance from the first day of embarking on this thesis. Our gratitude is also extended to our examiner, Prof. Riccardo Scandariato, for his positive feedback throughout the thesis. We would also like to take this opportunity to sincerely and with gratitude, say thank you to the Swedish Institute (SI) for having awarded us the Swedish Institute Study Scholarship that made it possible for us to have this education.

Faustine Nyangira, Marvin T. Ngoma, Gothenburg, August 2016

I would like to express my sincere gratitude to my wife Roswita Maarifa for encouraging me spiritually and for her passionate input throughout my masters studies together with my lovely son, Austin, and daughter, Audrey, for their continuous cheering and ambition to see me complete my studies. Nevertheless, my very profound gratitude goes to my family members and my thesis partner Marvin Ngoma who has been a friend not only during this thesis but since the start of our masters programme, sharing common views and helping each other throughout the programme.

Faustine Nyangira, Gothenburg, August 2016

I dedicate this thesis to my family, mom, dad and my sister, who have been extremely patient, encouraging and full of support throughout my education. I would also like to say thank you to my partner, my friend and a brother, Faustine Nyangira, whom I spent the most time with during my masters studies. Your encouragement and positive words always gave me the drive not to give up in tough times.

Marvin T. Ngoma , Gothenburg, August 2016

Keywords

Confidentiality:- the ability of a system to allow the disclosure of confidential information to only legitimate/authorised user(s).

Integrity:- is the ability of a system to prevent an unauthorized modification (altering, deleting, changing) of information or system's asset(s).

Availability:- the ability of a system to deliver expected service(s) to its legitimate users.

Maintainability:- the ability of the system to undergo modifications and repairs by either it self or by a third part.

Reliability:- the probability that a system performs a specified service throughout a specified interval of time under certain environment.

Safety:- the capability of the system to avoid catastrophic consequences on user(s) and/or the environment

Contents

List of Figures

List of Tables

1

INTRODUCTION

1.1 Background

The revolution of information communication technology has changed the way people do things. Today's technology is enabling us to do things better, faster and in smarter ways by way of how we access and interact with the information. This evolution has also been extended to the Internet, where anything that can be connected is on the Internet and can be accessed from any part of the world by various users with diverse backgrounds and different purposes. As a result the Internet now has a large number of devices that are interconnected and generating large amounts of data. This rings a wake-up call for possible attacks and security considerations when utilising technology.

Many organisations are currently implementing different security measures to secure their systems, controls, security mechanisms and processes and procedures. But a valid question could be "how secure are we?" or "how can we measure the security posture of an organisation, processes and procedures, security policies and/or computer systems?. A famous quote from Lord Kelvin says "I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind". These notions can be applied to information security to emphasise how important it is to measure security in order to know its posture be it in an organisation or in a given computer system.

Security metrication is expected to guide organisations in their approach to security management and help them deal with security in an appropriate way for their operations. Various approaches are now being used to measure security in order to have insight into the security status of IT systems, controls or processes. The security metrication concept is also used as a tool to facilitate decision making and determine the efficiency and performance as well as the security posture of an organization, including its IT systems.

Mell *et al.*[1] suggested that security metrics can be categorised in a number of ways. This generally can be done by considering those metrics that represent the maturity level of processes that are considered to enhance the security of the system, and those that represent the extent to which certain security characteristics are present in a given system. Most of the research [3, 4, 5] largely involves measuring the qualitative actual security state of a system that requires subjective evaluation based on a specific organisation's objective(s) and may not necessarily suit other organisations. As [4] suggests, some organisations differ in information metrics implementation depending on whether they are government or the private sector. In most cases, government organisations are policy oriented while the private sector is profit oriented and this is often reflected in the manner in which their respective IT security measurement programmes are designed.

1.2 Problem Definition

Security measurement is carried out for various reasons:- from ascertaining the security requirements fulfilment of computer systems; measuring the efficiency of processes and procedures within an organisation; to meeting legal and regulatory requirements, among others. With these varying objectives comes a variance in approaches and methodologies used when measuring security.

Having many approaches of measuring security means that there is no universal systematic way of carrying out measurement of security. This entails that each approach and/or methodology defines its own way of determining the various facets involved in the measurement process e.g. the decision criteria on what type of scale to use during the measurement phase or how to quantify the parameters of the security attributes that are measured [1, 2]. Also, the types of ratings and scores used in a security metrication activity may not explicitly give details on the criteria used to do the quantification.

Given the current state of security measurement, there is need to investigate the scientific soundness of suggested models. The criteria used to arrive at the various approaches and methodologies must be thoroughly checked and given a critique in order to justify them. Further, given that not all selection criteria within a suggested approach/methodology may be scientifically correct, there is need to find means of having a measurement process that incorporates the scientifically sound practices in its approach.

1.3 Scientific Contribution

This study presents a combination of measurement models with respect to the metrics used. A more exact and focused security measurement process is suggested. This is after careful consideration of the approaches and methodologies used in industry, research and standards and their scientific accuracy and/or effectiveness with regard to security measurement. We draw some conclusions on how a more comprehensive and/or specific metrication method must be defined.

The project also results into a suggestion of an approach towards measuring the security of an entire system. Various works have shown how difficult it is to accomplish this due to the multifaceted nature of security. After a deeper understanding of security measurement methods, approaches and metrics, we argue and propose a framework/steps to measure security and metrication. We also argue on some fundamental contentious properties of metrics such as quantitative vs qualitative; subjective vs objective etc and propose how they should be considered in the process.

1.4 Limitation

This research is based on literature review and interviews. Unfortunately due to time limitations and willingness of some companies to accept interviews on the topic we only managed to interview five companies. It could bring a better insight if at least 10 companies were interviewed.

1.5 Delimitation

Our research does not propose new quantitative or qualitative metrics. Instead we suggest a framework and guidelines that can help the process of measuring security and metrication in a systematic way. We still believe the arena needs more research on measurement and metrics formulation.

The rest of the report is structured as follows: Section 2 will explain the methodology we followed through this research from literature reviews and interviews conducted. Section 3 is gives some background regarding metrics, measurement and their properties. Section 4 gives the insight from the literature review while section 5 focuses on the standards with regard to metrication. Views from the interviews will be introduced in section 6. Section 7 will describe our proposed model for security measurement and lastly we give a summary, discussion and conclusion in section 8.

2

METHODOLOGY

2.1 Outline

This project has taken the approach of conducting a literature review on works that have been done around the area of security measurement. This approach was chosen to allow us to identify what is already known around the topic under research. In doing so, we aim to come up with questions that various works are yet to answer and also make a case as to why it is important to answer these questions. We will manage the results from the reviews by categorizing them into relevant parameter areas, and thereafter digest and give some thought to the literature under review.

We started with papers, books and journals that explain various ways of measuring security and/or metrics formulation. The common and prominent standards that were known to us included CVSS, ISO 27000 series and Common Criteria, among the others. These were directly searched from known sources. Other papers and journals were found in "Google scholar" by using the search terms: (information security measurements) OR (security metrics/ metrication) OR a combination of the two. This preliminary search brought 257,000 results that included books, journals and other published materials. Adding the keyword "information security measurement metrics" refined the search. With this number of papers, books and journals, we manually looked at the titles and selected papers with terms such as 'taxonomy', 'framework', 'models', 'approaches to measure security or 'security metrics' as keywords. We then looked at common applications or systems with regards to software, networks and/or of related terms. The resulted list had 2780 papers. We then chose potential papers based on the abstract and introduction sections that gave a direction to our thesis and found 270 papers. The final refinement was based on the keywords and areas that we focused on, to see how different stakeholders dealt with how to come up with a solution/contribution to the area. This included looking at aspects such as input parameters, scales and units used, security models, mathematical formulation, whether the metrics are subjective or quantitative etc (refer to section 2.3 for a detailed selection criteria). We eventually ended up with 72 papers to focus on.

Apart from literature review, we will supplement the information collection by conducting company interviews. A few companies that are involved in security assessment will be interviewed in order to get an insight on how they execute security measurement and also to find out how metrics are arrived at in the process.

In order to accomplish the stated outcomes, the thesis project work will be split up into the following parts:

1. A pre-study of various papers that focused on security measurement. The aim of this step is to establish fundamental facts about security metrics and also to clarify on some theories around the subject area. This step is vital in order to help understand how various stakeholders define *measurement*, *measures*, *metrics* and *metrication*, among other terms, in relation to the measurement of information security. See paragraph 2.2 for more information.
2. Review of research papers with the aim to find out what researchers are contributing towards the area of security measurement. Our focus is on what approach(es) they use/suggest in the derivation of various metrics to be used for the measurement of security. Paragraph 2.3 gives more details about this review.
3. Review of industry adopted standards for measuring security. The focus here is to understand the measurement methodologies used, input data, output metrics, mathematical approaches, among other aspects. See paragraph 2.4.
4. Review what approaches private and public organisations are using in order to measure security of their systems and organisations. The aim is to have an understanding of what some organisations in industry are actually doing in order to have a measure of security.
5. Conduct interviews with companies that carry out measurement of security. Our focus is on security consultancy companies as well as companies that offer products in which security is an important factor. See paragraph 2.5.
6. Identify any patterns or parameters in the various approaches and methodologies highlighted in the steps above, and categorize these accordingly. Some examples could be input data, scales used, measurement methods, etc.
7. Carry out an evaluation and analysis of the results of step (6) above and draw some conclusions on how a more comprehensive and/or specific measurement method must be defined.

A summary of the steps described above is shown in figure 2.1.

2.2 A Pre-study of the Literature

The pre-study was conducted by targeting papers that were accepted to a conference with regard to security. These were papers whose topic of focus was in the area of *Security metrics*, *Security Metrication* and *Security Measurements* or a combination of any of the three and the like. The culmination of this step was a set of papers that were published by university presses, by professional organisations and by well-known publishers. Thereafter, we sought to review reports from key workshops and seminars whose focus was on *security measurements, scores and rankings* as means of metrication.

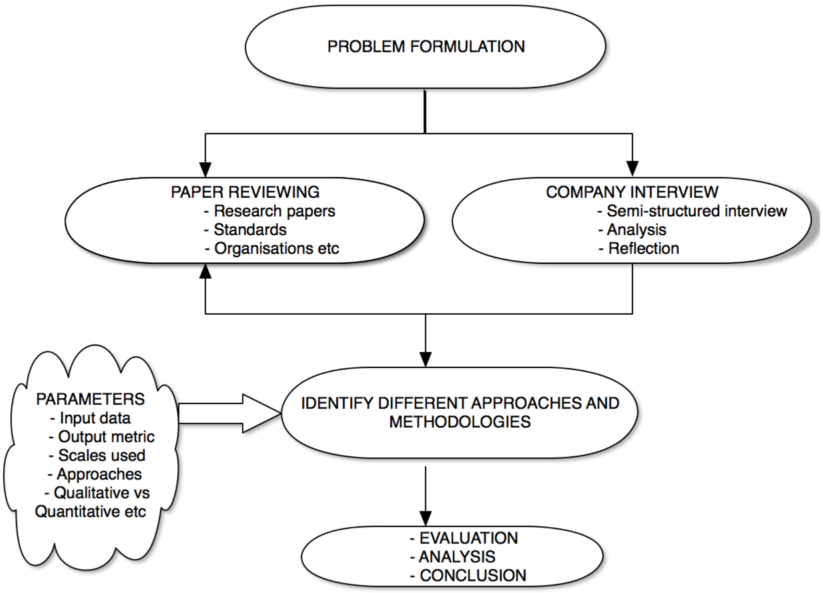


Figure 2.1: A diagram showing an approach to the thesis

These papers served as the source of the information for the sections labelled as research work, standards and organisations in the proceeding sections of this report. As already stated, this step was crucial in understanding the whole concept of metrication, metrics, measurement, measures and related terms with respect to measuring security and their importance with regard to security.

2.3 Review of Literature from Research papers

Carrying on from a generic literature review, our focus was now on various research works that had a contribution to security measuring. We looked at different approaches and methodologies being applied on various computer systems and the rationale behind them. This was done by searching different research works in the area of measuring security, security metrics formulation and other related works that could contribute on the matter. We expected the culmination of the set papers will bring about a wide insight on the matter and narrowing the scope is inevitable. This was done by reading either the abstract, introduction or discussion and introduction; or their permutations to get the insight of a paper. The main task is to analyse different views on the methodologies and approaches to measure security on the approaches used. On the later we focused on the top-down and bottom-up approaches which are mostly used in developing the metrics for measuring security. We reviewed these methods and suggest the better based on the advantages in the state-of-the-art.
We then looked at different methods used to measure security. A lot of papers were found and we focused on those papers that were clear on the following factors:

1. The Frameworks or benchmarks used if any for measuring security

2. The formal steps followed (if any)
3. The models used to help the process
4. The standards used.

Applications and users of the output result in measurement was also considered in the research. We strongly believe security is crucial because of critical information and human protection. Users with different roles are probably going to be beneficial to these measurements for mitigation and decisions making. So we looked at different works on application of metrics and mapping of roles and usage of metrics. This include executive officers, technical users with different speciality and system users among others.

A lot has been found regarding metrics. Different works gave different views and approaches towards metrics formulation. We looked at the following keywords and area of interest in the papers and this was our evaluation criteria on which we considered the literature to be reviewed:

1. Input parameters used
2. Type of scales or units
3. Security Models used if any
4. Definition of security prior to metric formulation
5. Subjective metrics and objective
6. Qualitative and quantitative metrics
7. Evaluation and validation of metrics and
8. Mathematical models/computation used for derivation of metrics.

We also summarize the literature review on research work according to the insight we got after gathering enough information from the research community. The summary will comprise all relevant aspects that seem important in metrics formulation and hence measuring security. .

2.4 Security Measurement Standards

Many organisations and bodies have put in a lot of effort in coming up with standard methods of measuring security. Some of these standards have been widely adopted by industry and form the basis on which the security of a lot of computer systems, products and organisational IT infrastructure is determined. Our focus was initially on the common standards including ISO/IEC 27004, CVSS and Common Criteria, as these provided detailed information on the methodology and approach they adopt in order to arrive at their measurements.

The three standards also have distinct descriptions with regards to some of the parameters we were trying to investigate. These included system modelling, measurement methodology, measurement scales used, mathematical approach and area of applicability. More aspects are also mentioned in the appropriate sections of this report. The scientific soundness of the methods and approaches is explored.

2.5 Company Interviews

In this section we present important points of note from semi-formal interviews conducted with security experts working with measurement of information security in industry. The goal of having these interviews was to gain practical insight into how security experts in industry carry out the measurement of security. Specifically, to look at how they measure security, methodologies and approaches used, and how they assess the performance and effectiveness of the adopted methods, approaches and metrics.

3

BACKGROUND AND TERMINOLOGY

3.1 Background

It has been inferred that security plays a big role in any organisation stemming from operations, management, processes to higher management such as board of directors as it influence the decision making to avoid turmoils, catastrophes and other disruptions in a business.

In this section we shall look at different definitions and descriptions of security terms with regard to metrics and measurement. Terms like measures and metrics are the most common terms that will be explained in details as understood from prominent stakeholders. Nevertheless, the properties and ambiguities in the methodologies and approaches to measure security or what makes a good metrics are also explained.

3.1.1 Measurements and Metrics

The two terms are often used interchangeably but there exists a difference between them. Payne [5] suggest that a measurements provides a single-point-in-time view of a given discrete factor while a metric is obtained by the analysis or comparison of two or more measurement taken in time. It has been observed also that measurements are mostly subjective while metrics can either be objective or subjective.

Rostyslav [6] added that a measurement quantifies a single dimension of an entity to be measured (e.g the number of intrusions detected by an IDS/IPS is 200) while a metric combines two or more measurements to reflect something that can be useful in decision making (e.g the number of intrusions this time is two times more than what was recorded previously or we have decreased the number of intrusions by 20%). The idea is not necessarily to express a measurement with respect to a similar measurement but having a value that could reflect something in decision making.

3.1.1.1 Measurements

Because measurements provide a single-point-in-time view of a particular factor, we can use two or more measures to derive a metric which can give the insight into the parameters measured and hence decision making. In addition to the definitions aforementioned, some stakeholders define measures and measurements as follows:

“A Measure is a variable to which a value is assigned as a result of measurement. Where a *measurement* is defined as a process of obtaining information about the effectiveness of Information Security Management Systems (ISMS) and controls using a measurement method, a measurement function, an analytical model, and decision criteria” [37].
“Information systems’ measures are the results of data collection, analysis, and reporting, which are based on, and monitor the accomplishment of, IS goals and objectives by means of quantification” [38].
George [7] defines measurement as an act or a process of measuring, where the value of a quantitative variable in comparison to a (standard) unit of measurement is determined.

3.1.1.2 Metrics

Unlike measurements, metrics are not obtained as a single-point-in-time values but through analysis or comparison of measurements taken over a period of time. The term security metric has been sporadically mentioned in many aspects, some of the views are represented below in rephrased quotes from [8]

“Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data”. The author tried to articulate the idea by considering the purpose of measurement in efficiency, performance or decision making by improving the measured activities or processes to suit the purpose the objective through observing the measurement outcome [39].

In [40], metrics are said to be quantifiable measurements of some properties of a system, product or other tangible property which has some attribute(s) regarding security. So a security metric of a systems or the combination of separate metrics of security attributes is a quantitative measure that a specific attribute possessed by an entity.

It can be seen that metrics are derived by comparing and analysing two or more predetermined baseline measures obtained over a given period of time. This is unlike measurements which provide single-point-in-time views of specific discrete factors [**?**]. This suggests that metrics can be obtained through analysis; subjective or objective or either qualitative or quantitative, unlike measurements, which are mostly quantitative and objective raw data. Moreover, in [8] they define a metric as a consistent standard for measurement with a goal of quantifying data to be able to facilitate the insight, improve efficiency and effectiveness through the analysis of pre-collected data [16, 50, 51]. The similar concept has been brought forward by [41] and shows the ability of a metric to act as a benchmark to the objectives set by an organisation. It can be revealed that metrics are important in facilitating decision making process and measuring security, the following sub-section explain the properties and qualities of a good metric.

3.1.2 A Good Metric

Having looked at what a metric is, our focus is now on establishing what characteristics, properties or qualities make a good metric. Different works from various stakeholders have come up with different views on what constitutes a good metric. Each property will be explained in a separate paragraph and summarized in the end.

In [5], they distinguish measurements and metrics by pointing out that a measurement has an objective value while it is not a mandatory in a case of metric (a metric can have either subjective or objective value). Joshua *et al.* [9] say that the area of security metrication strives to come up with an objective and subjective basis for measuring security. The same has been emphasized by Dr Gary Hinson [10] when listing the myths about metrics by saying that metrics should be "objective" and "tangible". Gary shows that it is easy to have an objective metric for tangible things but for intangible things like security we should put more effort into subjective factors rather than relying on some few irrelevant objective factors.

Metrics have different applications and benefits to an organisation including determining security posture and trends in an organisation, providing security accountability, justifying security spending and decision making among other benefits. It has been suggested that security metrics can be costly to implement, maintain, or develop but they needn't be [4-9]. Rostyslav [6] also suggests that the cost of metrics should be cheap/easy enough to be obtained to reduce the overall cost of other processes in an organisation which relate to security measurement in order to attain return on investment (ROI).

Quantifiable metrics have been proposed by many stakeholders as a means of having a good metric [6, 4, 8]. However, in [10] the same does not seem to be mandatory in order to derive a good metric especially when the purpose of the metric is to provide performance or effectiveness of a subject under measurement. For example, if someone wants to know how vulnerabilities in a system have been reduced from a previous measurement, saying 30 % of vulnerabilities have been reduced could yield a clear picture on the matter than mentioning the number of vulnerabilities found. In [4], qualitative metrics were listed to be accepted and this could be viable as most of them are used by the state-of-the art. According to Blakley [42], it is impossible to manage information security investment without being able to quantify it; but it's not necessarily to be the case. So whether the metric is quantifiable or qualitatively derived it should defeat the purpose of its objectives.

"You can't manage what you can't measure and you can't improve what you can't manage", this was a quote from [4]. The idea is to measure and have a metric that we know its purpose, intended users and how to report it. The output metric should be able to show its impact in improving the desired purpose and become manageable. The same has been said by [8] but phrased to mean "correctness and effectiveness" meaning that metrics should be able to do what the stakeholders projected them to do and meet the intended objectives without postulations to avoid ramifications in the system/organisation. Rostyslav *et al.* [6] suggest that "metrics should measure and communicate things that are relevant in the specific context for which they're intended and being meaningful". In [4], the idea has been simplified and stated that a metric should have a purpose and must answer the question.

Monitoring security of a system is a continuation and progressive process, the security responsible personnel is compelled to implement, maintain and review the policies, standards and procedures that people or system should adhere to. Measuring security should also consider these factors as a target system might change its properties with time. Payne [5] mention that a good metric should be "S.M.A.R.T", which means that it should be; **S**pecific, **M**easurable, **A**ttainable, **R**epeatable and **T**ime-dependable, the latter emphasises this property which is achievable if the metrics are repeatable. Adam [4] explained about metrics being repeatable and enhance the decision making process which is possible if temporal effects in the target system are taken into consideration. However, Rostyslav [6] shows how important it is to consider the latency of metrics with respect to the frequency and timeliness of measurements to avoid the metric deduced being inviable. Discrete measures are a bit easier to measure and manage compared to continuous values [10]. A good metric should take into consideration the effect to avoid the defeat on its purpose when a measured entity has a temporal property.
So, in summarizing, some of the properties and qualities that a good metric must have should include the following:

1. Could either be subjective or objective
2. Easily obtainable
3. Quantitative metrics are better but Qualitative are acceptable
4. Should have a purpose
5. Repeatable.

3.2 Other Factors to be Considered when measuring Security

In this section we identify other factors that should be considered when measuring security and deriving metrics. There is need to consider external factors that could contribute towards subversion of system's intended functionality. The concepts of reliability, maintainability and safety are introduced and their effect to security.

Apart from security attributes (CIA), other factors that affects security should also be considered in measuring security and metrics derivation. We mention these factors as dependability factors which include Availability, Reliability, Maintainability and safety (ARMS). We define these terms as follows:

As depicted in figure 3.1, Burtescu [48] suggested that security attributes are related to each other, so a failure of one attribute might have an impact on the other. Consider a system which is not secure due to breaches in confidentiality or integrity, this system can be reliable if there is no attack or threat imposed to subvert system's functionality. Therefore, a system can work under minimal security if it is reliable and there is no attack imposed, i.e, reliability of the system + no attack = security. Also availability depends on the reliability and state of a system with regard to a threat (even though there is no security), so , reliability + no threat/attack + no security = availability. It can be inferred that the attributes of security are dependant on each other. This concept should also be considered when designing a secure system or model as depicted in figure 3.1: *no reliability -> no availability -> not secure*

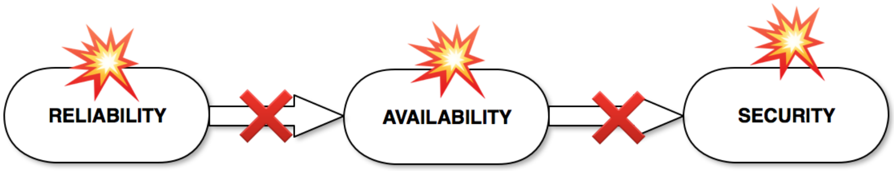


Figure 3.1: Relationship between security and dependability attributes

The two aspects (security and dependability) can be separated as:

1. Preventive measures which represent the input characteristics to a system or the ability for a system to resist environmental influences that can be introduced to a system as a security breach.

2. Behavioural measures which represent the output characteristics which shows how the system behaves after breach introduction to a system.

Identifying different factors that can affect security and hence its measurement and metrics formulation, it is better to have the conceptual security model that exposes all the possible threats by combining the CIA and ARM attributes. For this purpose we propose using a threat model that will help identifying possible attacks) to a system. The OWASP define a threat model as an approach for analysing security of an application by identifying, quantifying and addressing possible security risks. Other companies like Microsoft [43] also proposed the following self descriptive threat modeling process.

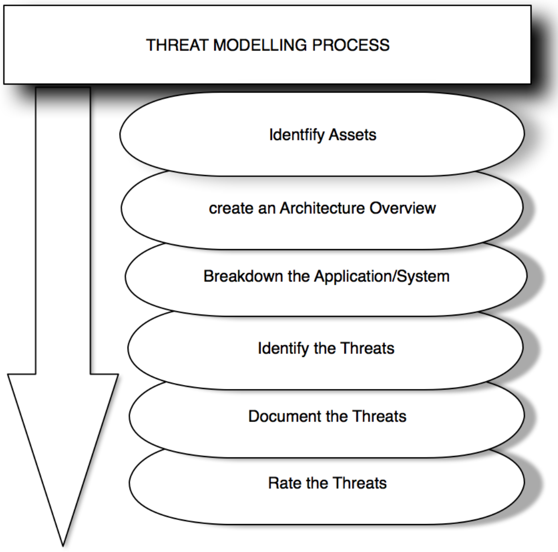


Figure 3.2: Microsoft threat modelling process

As shown in figure 3.2 , the analyst should consider threat modelling process when rating and identifying the threats that are possible to affect the system. The haphazard manner of securing a system is not enough to give a confidence that a system risk free. Having the idea that "until you identify threats, your system is not risk free and secure" will help prioritizing threat models. The first step in the model is to identify valuable resources that should always be protected and create a formal architecture of an application, system or environments prone to vulnerabilities. The breakdown of a system or application exposes the possible interactions to and fro the application. This will make easy the process of identifying threats for model designing and documenting easier. The final step helps to identify threats of high risks which need appropriate and immediate mitigation.

4

A REVIEW OF RESEARCH LITERATURE ON SECURITY MEASUREMENT

4.1 Preamble

Under this section, we shall look at different journals and other academic work under the area of security metrication and measurement and see how the ideas will fall under the purview of this study. As already explained in the methodology section, we will start with different approaches for measuring security and metrication. The two terms (measurement and metrication) will be used side by side as metrication plays a vital role in knowing the posture of security in a system or organisation. Then we will combine these ideas to enunciate a clear picture on a framework and steps that should be taken to foster the design of security metrics and security measurement.

4.2 Approaches to Measure Security

Depending on the objectives of an organisation, measuring security and designing a metric could involve different steps/approaches. The process could involve identification of some key points like knowing sources of input data, the objective of measurement/metrics and other methods that should be followed [8,11]. Jennifer *et al.* [12] describes the GQM approach which suggests identifying **G**oals, asking **Q**uestions and design a **M**etric as an approach to design a metric and measure security. The approach could can be done recursively in order to get metrics that can exactly serve the purpose. It will be explained later how challenging it is to obtain metrics or measures for an entire system that comprises of many sub-components. As Jonsson *et al.* [14] suggest, it is not viable to know the security of a system as a whole at all times but in some cases, measuring individual attributes constituting the system could be of great importance.

After having procedures or guidelines for measuring security, a top-down or bottom-up approach could be used to fine-tune the metrics to be used. Rostyslav [6] suggests the two approaches with a hint that one could be better than the other though it also depends on the type of system under measurement and the objectives or goals of the measurement.

As depicted in figure 4.1, Payne [5] proposed a top-down and bottom-up approaches towards metrics formulation. According to Payne, a top-down approach tends to readily derive metrics that will exactly serve the purpose of the pre-set objectives while the bottom-up approach derives easy and simple metrics. A top-down approach allows the lower-level objectives to be derived and fulfilled while the bottom-up approach helps to be precise on what to focus on during measurement/metrication [6].

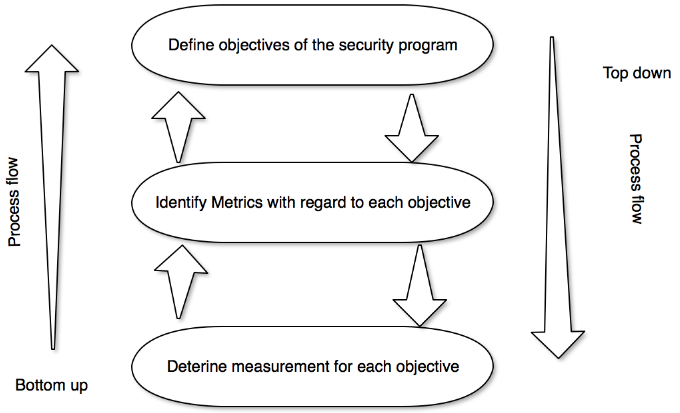

Define objectives of the security program
Top down
Process flow
Process flow
Identify Metrics with regard to each objective
Deterine measurement for each objective
Bottom up

Figure 4.1: Top-down versus Bottom-up approach to measure security

Rostyslav [6] gave an example of the evaluation done for DOD Air force, and NASA Jet Propulsion Laboratory (JPL) on the approach used for measuring information security (IS) metrics. It was observed that the top-down approach used by JPL was more successful compared to the other approach (bottom-up) used by other companies. This is because the latter approach ended up requiring a lot of data to be linked up to higher level objectives.

Deriving metrics involves analysing different measures and comparison among them in order to get an insight in decision making. So gathering information is one among the crucial steps in metrics formulation. Some suggested methods for data/information collection [16, 37, 3] are: patch management system, risk assessment results, network scanning systems, incident reports, vulnerability scans e.t.c.

A security model or a security threat model can be helpful in identifying possible threats and breaches that might have an impact on a system. However, Many companies and organisations either do not have professionals for security metrics formulation or perhaps do not have enough insight on the topic [44]. As a result, it is not the norm to find development of frameworks or models which provide an easy and simple guidance for measuring security and obtaining metrics. Some works that came up with frameworks such as [15, 13] seem to be helpful in identifying requirements and inputs to the process. For example in [15], the framework mentioned

4 steps for getting metrics for cloud computing security as; metrics identification, threat identification and analysis, threat processing and application of the metric evaluation by decision makers.

The idea of how to devise security metrics was also adopted from the concept brought forward by Voas [30]. Voas suggested that the security of a system comprised of sub components C1 and C2 can be deduced by considering the security of the two components separately. However, the impact of an incident on component C1 could be different from that on component C2 under the same incident.

For mobile ad hoc networks (MANETs), the same concept has been considered and summarized as follows:

1. Defining security objectives: Which depends on the assumption to the possible threats by considering the environment and the required security level
2. BMCs (basic measurable components) selection: Depending on the above objective(s)
3. Identify other dependencies between different attributes (called BMCs for this case) that might be the source of vulnerabilities. Re-defining these BMCs might also be possible.
4. Identifying the integrated composition of the system. This can be used to form metrics and hence measure security either quantitatively or qualitatively.
   MANETs identified areas that can be used to estimate security levels along with heuristics helping the development of metrics for measuring security as indicated in table 4.1. More details can be found in [25]

4.3 Security Metrics

4.3.1 Designing a metric

Other contributions to the field of security metrics suggested a list of steps that are useful when designing security metrics. Kristoffer [16] mentioned some useful steps which can help designing a security metric as follows:

1. Select the control for which a metrics should be designed for.
2. Select a first semi-formal interview to gather data and requirements
3. Design first version of a metric
4. Conduct a second semi-formal interview to fine-tune to previously design metric.
5. Finalize the metric
6. Perform measurement using the designed metric
7. Perform aggregation using the gathered data and create a report.

The similar steps for metric designing with a little twist are given by Payne and Nichols [45, 5] as: objectives definition; determine information goals; develop metrics models; determine metrics reporting format and schedule; implement metrics;

Table 4.1: Metrics development for Sub-components

Component	Sub-component	Heuristics
Cryptographic metrics	cryptographic strength	CIA of messaging, payload data and meta-data in general
Trust metrics	Initial trust metrics	Initial trust is based on reputation information
	Operational trust metrics	Operational trust value depends on the context, detected suspicious activities and up-to-date threat data
Routing security metrics	Routing data	CIA levels of routing data, application of cryptographic metrics
Mobility security metrics	Identity data	CIA levels of ID information
	Packet forwarding data	CIA levels of forwarding data
Human factors andperformance	Usability	Usability and user experience metrics
	Performance metrics	Performance metrics, security performance metrics
Quality metrics	Functionality	Functionality and availability metrics
	Reliability	Reliability metrics
	Efficiency	Efficiency metrics, security solution efficiency metrics
	Maintainability	Maintainability metrics
Exposure metrics	Scalability	A system is more exposed to a threat when it is larger or there are more nodes
	Probability	The system is more exposed to a threat when the threat probability becomes higher
Other metrics	Other factors	Privacy, dependability, robustness, survivability, legislation and regulation implications, cultural issues etc

set benchmarks and targets and establish a formal review cycle.

Having an objective still seems to be helpful prior to formulation of metrics or measurements. The aforementioned steps would be necessary in forming a metric but they should be flexible depending on the type of metric to be designed and the organisation's objectives or usage of those metrics. A simplified framework for measuring security will be introduced in section six (our proposed model for measuring security).

Sademies [28] suggests that metrics can be used in an organisation for different purposes and by different people including executives, information security teams, network infrastructure teams; hardware and software technicians; and risk analysts. The idea of having guidelines for metric formulation is vital. Sademies' work, with adaptation of ideas from Payne [**?**] presents the following guidelines for metrics formulation and measuring security:

1. Identifying metrics' objectives
2. Decide type of metric to generate
3. Develop methods for generating metrics
4. Setting the targets for development of metrics to reflect the objectives
5. Find a way to report metrics
6. Create plans for acting on the developed metrics and
7. Establish refinement of the developed metrics and reviewing (this might involve iterating the above steps).

4.3.2 Properties of a Metric

Wang *et al.* [26] gave guidelines on information security metrics by explaining the four axioms properties that a metric should have as described below.

1. The same measure should not be assigned to all systems, i.e systems with strong secure applications will run in higher level of security than those with normal secure applications.
2. Systems with the same security level or same class should have the same or equivalent security measurements.
3. Different metrics can be assigned to the same system(s), for example two virtual machines with the same security configurations can have different metrics depending on the user using the system, i.e whether the user is pro (or hacker) or a normal user.
4. The measure should have a different impact depending on the ordering of subcomponents, for example placing a demilitarized zone in front of or behind the servers should have a different impact on the overall outcome of the measure/ metric.

Other properties of a good metric can be found under section 3.1.2

4.3.3 Classification of Metrics

Savola's [25] work focused on a survey from governments, industries and academics and came up with a taxonomy of security metrics in the research and development (RD) arena. The development of high-level security metrics helps to derive other composite metrics for various systems including complex systems and aids the process of decision making in engineering processes as well as business. In this work, metrics were classified into three categories namely business; information security management in organisations and; ICT products, systems and services as follows:

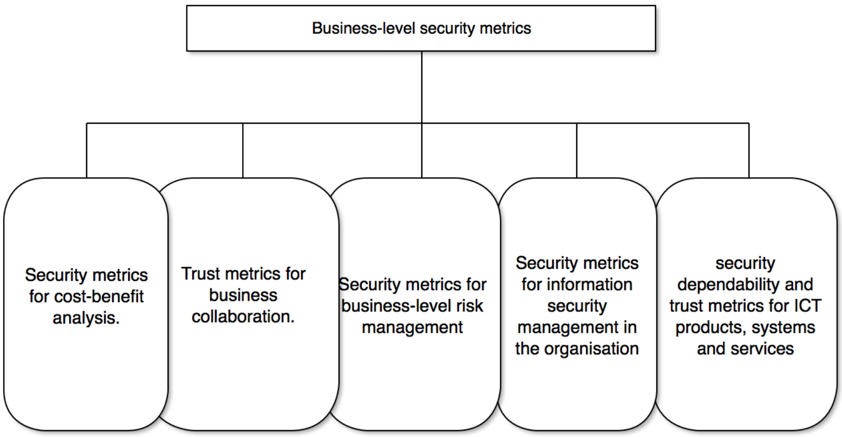

Business-level security metrics
Security metrics for cost-benefit analysis.
Trust metrics for business collaboration.
Security metrics for business-level risk management
Security metrics for information security management in the organisation
security dependability and trust metrics for ICT products, systems and services

Figure 4.2: Business level metrics [25]

- **Business Level Security Metrics**: Metrics are designed according to the objectives and goals of a business. Different areas that have to be looked at when deriving metrics are shown in figure 4.2.

- **Metrics for Information Security Management in Organisations**:These are metrics that could be used for ISM (information security management) which comprises of metrics to support evaluation of security plans, controls, certification and accreditation activities [25]. The arrival to these metrics has adopted some standards of measuring security. The classification of areas and their corresponding metrics usage are depicted in figure 4.3.

Operational metrics addresses the three sub-components (i.e susceptibility and effectiveness) and focus on achieving up-time of software, hardware and controls. Other related informational equipment and their evaluation in meeting security targets are also included in this category. Technical security metrics are adopted from NIST SP 800-26 [33] for security assessment with the help of NIST SP 800-53A [33]

- **Security metrics for ICT Products, Systems and Services**:The basic concept of this taxonomy was from the study by Avizienis *et al* [31].The metrics were further categorized into metrics for life cycle management, security assurance and security engineering. Figure 4.4 shows the breakdown of the categories. A reference to the details of the subcategories can be found in [31].

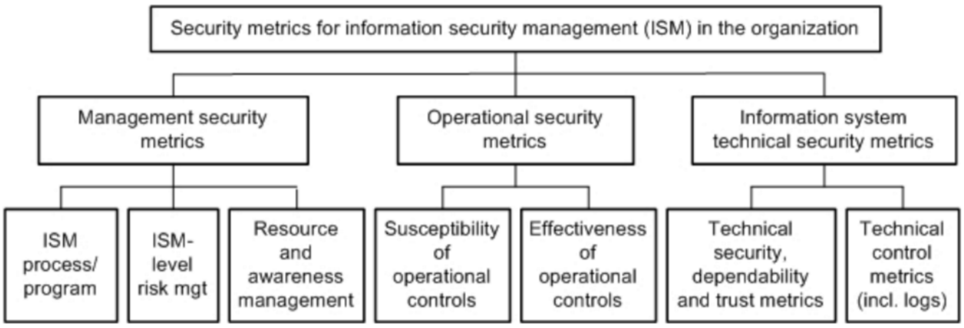

Security metrics for information security management (ISM) in the organization
Management security metrics
Operational security metrics
Information system technical security metrics
ISM process/ program
ISM-level risk mgt
Resource and awareness management
Susceptibility of operational controls
Effectiveness of operational controls
Technical security, dependability and trust metrics
Technical control metrics (incl. logs)

Figure 4.3: Metrics for Information Security Management [25]

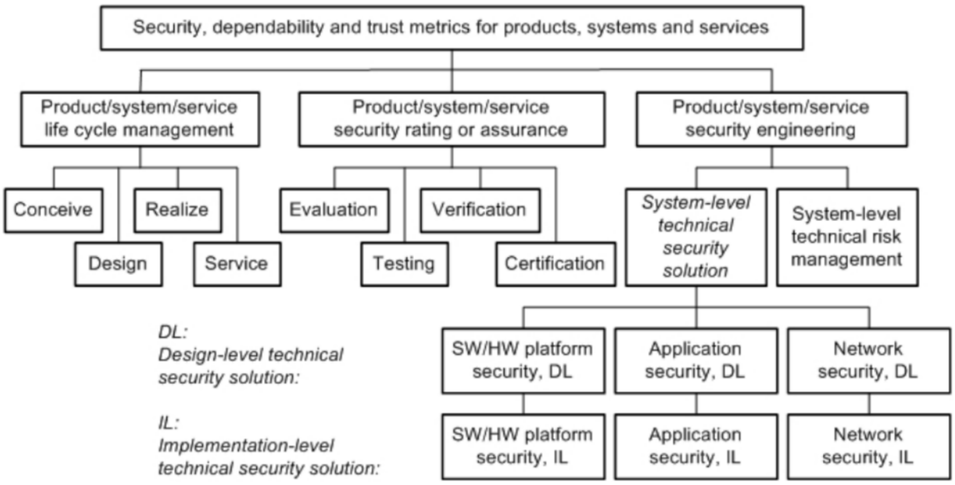

Security, dependability and trust metrics for products, systems and services
Product/system/service life cycle management
Product/system/service security rating or assurance
Product/system/service security engineering
Conceive
Realize
Design
Service
Evaluation
Verification
Testing
Certification
System-level technical security solution
System-level technical risk management
DL: Design-level technical security solution:
IL: Implementation-level technical security solution:
SW/HW platform security, DL
Application security, DL
Network security, DL
SW/HW platform security, IL
Application security, IL
Network security, IL

Figure 4.4: Metrics for products, systems and services [31]

Patriciu et al. [22] present two types of metrics (metrics in this section are used in the process of measuring the security of a component); metrics to evaluate vulnerabilities and metrics to evaluate system controls as described below:

1. Metrics to Evaluate vulnerabilities: In this type of metrics, the work relied on CVSS (Common Vulnerability Scoring System) to derive the overall composite scores for measuring the severity of a system with regard to vulnerabilities.The derived metrics were either qualitative or quantitative. The details on *temporal*, *base* and *environmental* metrics from CVSS is explained in the " STANDARDS" section of this report.

2. Metrics to evaluate information systems security controls: To evaluate controls in information security systems, the following inputs were considered.
   (a) **Definition of security**: The focus of security attributes used under this section are integrity and reliability.
   (b) **Type of system**: The considered system for metric formulation is a network system.
   (c) **Input data**: In order to form a metric, different data items were collected from different sub-systems including security bugs, network scans, rate

of software application bugs and other reported bugs.

The process of deriving metrics depends on the type of incidents that organisation's assets are prone to their effects. The process starts with incidents identification to the respective controls in the system, then metrics can be derived as shown in figure 4.5.
The types of metrics are also grouped into categories depending on the usage and role of users as summarized in table 4.2. A few examples are mentioned here and the detailed explanation can be found in the referenced paper.

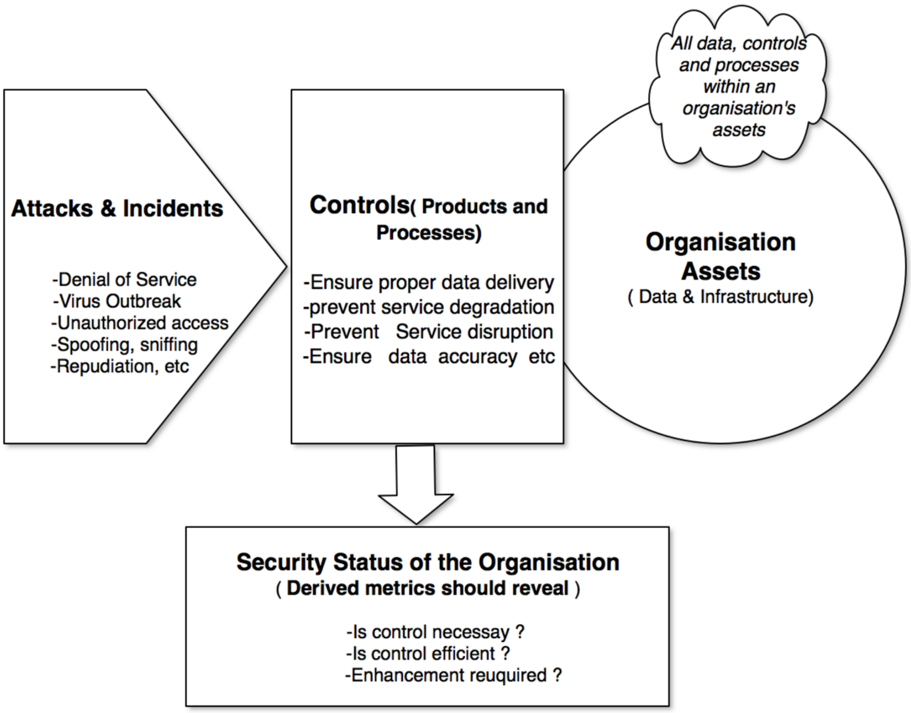

All data, controls and processes within an organisation's assets
Attacks & Incidents
-Denial of Service
-Virus Outbreak
-Unauthorized access
-Spoofing, sniffing
-Repudiation, etc
Controls(Products and Processes)
-Ensure proper data delivery
-prevent service degradation
-Prevent Service disruption
-Ensure data accuracy etc
Organisation Assets
(Data & Infrastructure)
Security Status of the Organisation
(Derived metrics should reveal)
-Is control necessay ?
-Is control efficient ?
-Enhancement reuquired ?

Figure 4.5: Network and systems security metrics[22]

Table 4.2: Metrics types and usage

Metric type	Executive officers	Network and IT systems operations groups	The network and security users
System Service and network Levels	YES	YES	NO
Business Requirements met	YES	NO	NO
Number and organisational impact of Comprises	YES	YES	Impact of Compromise (YES)
Peer performance	YES	NO	NO
Packet losses, Network Performance, Throughput and Utilization	NO	YES	NO
Viruses Detected and Unauthorised access	NO	YES	Unauthorised access (YES)
Intrusion Attempts	NO	NO	YES
Suspect Port Scans	NO	NO	YES

NB:
Executive officers: These are personnel that are responsible for the overall business or organisation operations and concerned with all information systems which help business continuity. Executive officers have the authority to relocate, hire human resources as well as funding the business.
Network and IT systems operations groups: These are responsible for the infrastructure and the overview of network and systems security. They are tasked to prevent, detect and act on security breaches and intrusions.
Network and systems security team: These are responsible for systems security policies and other programs that need attention with regard to security.

Anni [19] carried out a research on the development and implementation of information security metrics in organisations in relation to literature in a research field. The research looked at other proposed classifications of metrics like Henning's [29] who proposed four categories; Technical metrics, Organizational, Operational and "brainstormers" metrics. Individual metrics that are concerned with measuring the awareness and expertise of users in an organisation together with environmental metrics as presented with their description as shown in table 4.3. Swanson *et al* [32] ideas on metrics classification was also considered and includes the followings:

1. Implementation metrics which are used to measure the implementation of security policies
2. Efficiency and effective metrics to measure the evaluate the implemented services and results

3. Impact metrics to measure the impact on business goals/mission of security incidents.

The detailed classification of metrics according to [19] is shown in table 4.3.

Table 4.3: Security metrics classification

	Technical IS* metrics	Organisational IS* metrics	Operational IS* metrics	Brainstorm IS* metrics	Individual IS* metrics	environment IS* metrics
Description	Technical object	Effectiveness of programs and processes of the organisation	Risks to operational environments including IS used systems and operating practises	Synthesis, cross-track issues and big picture concerns	Individual expertise	Security aspects of the environment of organisation or operation
Example	Logs	percentage of systems accredited	Asset values	Combination of Technical, organisation and operational IS* into one framework	Awareness of educational level of an employee	Threats caused by functioning in certain environment
Challenges	May contain a lot of useless data, often used to be filtered and rationalised	Require viewpoint of the whole organisation, not necessarily directly applicable in other organisation	Require that the operational environment and its effects are understood, this can often be just assessed	Require viewpoint of the whole system life cycle	Difficult to level on the organisation scale	Possibly difficult to model function of an environment, can contain unexpected factors and combinations

4.3.4 Use of Metrics

Metrics can be used in many area with different purposes. Kajava [24] pointed out some few applications as follows:

1. *Objective establishment*:The company could have goals to establish in terms of business (so knowing the posture of an organisation could be important before starting new projects) or goals and targets with regards to systems' operations and security.
2. *Prediction*: Metrics can be used to predict security achievements on the implemented systems, processes and controls in an existing system.
3. *Comparison*: Comparing different security levels of technical systems/objects.
4. *Monitoring*: Can be useful to monitor the security level of an object through the pre-determined benchmarks.

Nevertheless, according to Wang *et al.* [26], metrics can be used to know the success of information security policies, mechanisms, processes, procedures and implementations to mention but a few. This can help security professionals not only to know the posture of security in an organisation or a specific product but also how and to what extent the systems are secure.

4.4 Steps to Consider when Measuring Security

In this subsection we look at different research works and find related parameters in the area of security measurements and metrics which leads to measuring security. Wang *et al.* [23] suggest that quantification still seems to be difficult to achieve all the time. Due to multifaceted nature of how we define security, it is suggested, instead, to measure the attributes of interest with regard to security in order to have a clear picture of how the system/component is secure. The work suggested a framework (called SM) that can be used to measure security of a computer system. The SM is divided into the following elements:

1. Definition of security
2. Selection of units and scales that will be used
3. Definition of an estimation methodology
4. Validation of measures

As outlined above, the description of each term is concisely explained below:

4.4.1 Security Definition

Because security is multifaceted, the definition of the term depends on the context and the types of system addressed. For example, security attributes used in stock exchange network could be real-time availability and information privacy (Availability and Integrity) while in an on-line newspaper integrity could be a suitable attribute to consider. So, security or its attributes should be defined with respect

to the system.A function
<f1(confidentiality), f2(availability), f3(integrity)>
can be regarded as a definition of security in three tuple with regard to CIA. When different aspects have to been measured, then a function can be re-written as:
<f1(confidentiality), f2(integrity), f3(availability) , g(f1, f2, f3)> where g(f1, f2, f3) = 0.65f1 + 0.1f2 + 0.25f3
which means the system has been defined as a dependant to 65%, 10% and 25% on CIA respectively.
NB:
The figures are given to a specific attribute in a ratio which depends on priority given to a specific attribute compared to another. The total percentage sums to 100%

Kajava *et al.* [24] in his research defined security with regard to measurement by considering three attributes, i.e confidentiality, integrity and availability.
However, Savola *et al.* [25] proposed an integrated security measurement framework for mobile ad hoc networks (MANETs) to help network-level decision making. A simple description of MANETs can be found in this paper. The following categories regarding the definition of security were pointed out.
The metrics were divided into on-line and offline with different usage, for example on line metrics' purpose is for decision making and on line monitoring while the offline metrics were used for adjusting on line measurement activities, prediction and improving implementation quality.

Due to nature of MANETs, its mobility and infrastructure less nature, identifying general metrics was not easy because the system is comprised of many subsystems and. So, devising metrics and measuring started with identification of threats using the table 4.4, then reviewing the security goals set for the MANETs, having the overview of security requirements and then focus on security metrics.
The definition of security for this work is: confidentiality, integrity, availability, authentication, authorisation and non-repudiation. Table 4.4 shows the possible threats and possible countermeasures that might be used to develop measures or metrics.

4.4.2 Selection of Units and Scales

Scales and units help to measure a system and simplify the interpretation of the results. Different scales like nominal, ratio, absolute and others could be used depending on the context and aim of measurement. A detailed explanation of these scales and units could be found from [23, 34]. When using a scale and units, the following should be considered.

1. *Plausibility*: How much information the scale is capable of revealing
2. *Accuracy*: The possibility of avoiding errors that might appear.

4.4.3 Measuring Method

A concept of how to devise security metrics and hence measuring security was also evolved from the concept brought forward by Voas [30]. Voas suggested that the security of a system comprised of sub-components, say C1 and C2, can be deduced by considering the security of the two components separately. However, the impact of an incident on component C1 could be different from component C2 under the same incident. More information is given in [25].

For MANETs, the same concept of considering components in measuring security has been considered and summarized as follows:

1. Defining security objectives: These depend on the assumption of possible threats by considering the environment and the required security level
2. BMCs (basic measurable components) selection: Depending on the defined objective(s)
3. Identify other dependencies between different attributes (called BMCs for this case) that might be the possible sources of vulnerabilities. Re-defining these BMCs might be possible too.
4. Identifying the integrated composition of the system. This can be used to form metrics either quantitatively or qualitatively.

MANETs identified areas that can be used to estimate security levels along with heuristics helping the development of metrics for measuring security as indicated in table 4.4.

Kajava et al. [24] suggest that measuring security becomes handy and more useful when metrics are derived from the collected/historical data analysis. The methods for measuring security were adopted from Jonsson (2015) [34] and the following were suggested:

1. Risk analysis : Which means the estimation of possible intrusions or anything that can endanger defined assets and their corresponding costs or consequences.
2. Certification : Classification of a system in classes with regard to its design or properties and security mechanism. Common criteria can be used to achieve this. (see section 5.3).
3. Measures of intrusion process: Based on the statistical measurement of the effort it takes to compromise a system. This can be argued because it is subjective and will depend on the skills of a user testing the hacking. Auditing was also considered as a way of measuring technique.

Nevertheless, Wang et al. [27] propose a new approach for the definition of security metrics and hence the measuring of security in software is done by considering the possible vulnerabilities according to CVE (common vulnerabilities and exposures) for the naming of common vulnerabilities and CVSS for mapping scores. Their research work can be categorised as follows:

Security definition: The work focused on security attributes from CVSS which includes but is not limited to confidentiality, safety, integrity and availability.

Type of system: This research work focused on a Software system. The focus was on individual vulnerabilities in an application and not the entire software system which might have multiple vulnerabilities. This is because of complexity and multi-

Table 4.4: Threats to MANETs [25]

Class	**Threat**	**Countermeasures**
Network threats	Active mode impersonation	Node authentication
	Message replay	Node authentication, message integrity
	Denial of service	Node authentication, session authentication
	Message copying and listening	Encryption
	Injection of erroneous messages	Node authentication, encryption
	Distributed denial of service	Node authentication, session authentication
	Message distortion	Message integrity
	Message deletion	Non-repudiation
MANET specific threats	Black hole attack	Node authentication, encryption, secure routing
	Route information manipulation	Encryption
	Old route information replay	Encryption
	Inefficient routing	Network management, efficient routing
	Excessive data load	Network management
Other threats	Virus	Anti-virus Software, updates, firewall, patches
	Trojan horse	Anti-virus Software, updates, firewall, patches
	Software bugs	Software updates, patches, security assurance activities
	Eavesdropping	Encryption, transfer media planning

dependant factors which might exist between different affected attributes and the overall implication on the system.
Quantitative vs Qualitative: The idea of having or formulating metrics is to get the quantification of security measures that could help to monitor, manage security and decision making. The research tried to come up with a quantification of these metrics but we can argue against this since the derivation used qualitative methods and all are subjective.
Mathematical formula for quantification:
Wang *et al.* [26] proposed a mathematical formula for quantifying metrics as follows:
Let;
SM- software security metrics
Wi (i=1,2,3 . . . ..,k) - Weaknesses identified in software (s).
Vi (I=1,2,3 . . . .,m) - CVSS scores on vulnerabilities Vi.
Pi (i=1,2,3,...,m) - Risk of the corresponding weaknesses found.
Ri (i=1,2,3 . . . .,m) - Frequency of occurrence of a given weakness
K - Number of weaknesses
M- Observation time (in months),
With the above definitions, the following formulas were deduced:

$$SM(s) = \sum_{n=1}^{m}(P_n * W_n) \tag{a}$$

This means a metrics (SM) is given by summing up the product of every weakness found and its associated risk. The weakness (Wn) in an application or a software is given by the average of all vulnerabilities scores or weaknesses found according to CVSS.

$$W_n = \frac{1}{K} * (\sum_{i=1}^{k}(V_i)) \tag{b}$$

$$P_n = \frac{R_n}{\sum_{i=1}^{m} R_i} \tag{c}$$

The risk associated with an application (Pn) is the ratio of the frequency of occurrence of the weakness to the sum of all weaknesses, where the frequency of occurrence of a weakness (Rn) is given by the ration of number of weaknesses to the time of weaknesses' observation.

$$R_n = \frac{K}{M} \tag{d}$$

It should be noted that the sum of all risks of the corresponding weaknesses is 1.

$$\sum_{n=1}^{m} P_n = 1 \tag{e}$$

4.4.4 Measurements Verification, Validation and Estimation

Estimating security attributes is not as easy as measuring aspects of a physical entity. Sometimes, estimation and qualitative measures can be used in order to have realistic results. Different approaches for estimation have been suggested in [25]as a reference for different attributes of security. However, after measurement, the result should preserve the aim of the measurement. It would be aspicious to have someone validate the results even though this may not be a simple task. In [25] some methods have been suggested as reference for an in-depth understanding.

Nevertheless, for measuring security and obtaining metrics, Wang et al [26] gave detailed guidelines for verification and validation of the results of the measurement. The work focused on measuring security implementations. As defined in the paper, a security mechanism is a tool or method used to enforce security policies and procedures. The failure in a security mechanism results in vulnerabilities. The suggested methods employed in a security mechanism include; formal verification, evaluation, assessment, direct testing, accreditation and observation of systems' performance. The verification is mainly done through the presence or absence of vulnerabilities. Formal verification was suggested as the best method while penetration was regarded as inefficient as it can be used to test for the presence of breaches and not their absence.

In formal methods, static analysis and model checking are the main types used and are described as follows:

1. *Static analysis* : Mostly used in compilers and interpreters especially during software validation and re-engineering where the properties of code is inspected in order to verify or optimize the code for security enhancement purposes. The idea is to neutralize some possible bugs before deployment of a software/ application.
2. *Model checking* : In model checking, the idea is to verify systems properties by using some logic steps with state transition in a system (application or software). So, if a system and its security properties are modeled it becomes easier to identify whether the state of a system or subsystem violets some security properties of the system.

4.5 Summary on Research Works

We summarise the insight into research works based on various aspects that are important in measuring security and for metrics formulation.

Table 4.5: A summary from the research work

Summary On the Research Work		
Aspects	Input From Research Works	Comments
Approach to measure security	-Depending on the objectives of an organisation, measuring security becomes easier when metrics are formed using a top-down approach which derives metrics that exactly serve the purpose of the pre-set objectives. The approach is suitable in both few and bulk input of data for analysis and measurement. -GQM (goals, questions and metrics) is another approach used to measure security and derive metrics. The approach involves setting goals for security measurement and metrication, asking questions regarding the input data and system under measurement and finally deriving a metric.	Other methods can be employed if and only if they seem applicable and favours the process' simplicity and objectives.
Designing a Metric	-Some steps have been suggested towards measuring security and metrics formulation as: -Select controls from which metrics have to be designed (or identify attributes to be measured) or identify objectives/goals of measurement. -Select a first semi-formal interview OR determine information goals which can be used to get more information about controls, processes or attributes. -Develop a metric model or first version of a metric -Finalize metric implementation and measurement using the developed metric. -Perform aggregation using the collected data and reporting -Establish formal review cycle for metrics formulation	It should be noted that some of the properties of a good metrics involve S.M.A.R.T as explained under section 3.2.1

Summary On the Research Work		
Aspects	Input From Research Works	Comments
Security Definition	-Different research works have considered security definition as a requirement for measuring security. -Most works define security in terms of CIA (confidentiality, integrity and availability. Others also extend to safety, reliability and non-repudiation as a definition of security. Security definition depends on the type of system to be measured, priorities and severity of attributes that could impact a system, component, processes or controls.	This is one among other fundamental steps in metrics formulation and security measurement. It gives the benchmark for objectives verification
Selection of Units and Scales	-Units and scales are used in both qualitative and quantitative measurement approaches. Scales like nominal, absolute, ratio, percentage, average are among the formal scales used.	Understanding the implication of each type of scale and unit before deciding which one to use is imports. Different scales and units have different capabilities and strength.
Type of a System	-Different types of systems are identified in order to be aware of possible impacted security attributes and awareness of possible measurable and considerable security attributes. -Some considered systems are network and software, also cloud computing and security policy awareness were subjects of interest	Some pre-known systems have guidelines on how to measure security and derive metrics. So identification of a type of system could smooth the process.
Input Data	-Depending on the type of metrics, different data can be used for analysis and metrics formulation after measures. -Some useful input data are: Risk analysis, network scans, penetration test, network and software incidents, security bugs, different logs etc.	Because metrication involves analysis or comparison of two or more data, populating a data-set is handy.

Summary On the Research Work		
Aspects	Input From Research Works	Comments
Classification of metrics	-Business level security metrics. -Metrics for information security management in an organisation -Metrics for ICT products (Common Criteria was used) -Metrics to evaluate vulnerabilities (CVSS was adopted) -Metrics with regard to user Roles in an organisation (executive, network and IT systems' users, network and security users etc) -	Depending on a type of systems/ applications available, processes and procedures, metrics can be classified accordingly. This makes the understanding and interpretation of the specific metric easier for specific people.
Qualitative or quantitative	-Most of works came up with qualitative measurements and metrics while there are few that are quantitatively derived and still used subjective methods in the process.	Either way can be used to obtain metrics or measuring security.
Application of Metrics	-Measuring security could have many applications including: -Objective and goals establishment with regard to business continuity decision, return on investment or security mechanism etc, prediction of security achievements, comparing different technical systems and monitoring security levels of an object, system or component(s).	Different metrics are used for different purposes.

As depicted in table 4.5, different parameters have been considered from the research work. We have considered only some parameters that are more relevant for our thesis. We have looked at different approaches used to measure security and the choice of which approach to use depends on the objectives and the expected outcome from the metrics or measurements. However, GQM and top-down approaches seems to be more common. Designing a metrics involves some schematic steps towards its accomplishment, most of the research works mentioned objective settings to be a vital step among the others. Reporting the metrics also seems to be obvious designing metrics because metrics should give the insight in security posture for decision making.

Metrics classification was also pointed in designing metrics and measuring security. Depending on the objectives set by an organisation, identifying the type of metrics to be derived could help to narrow down the scope of deriving metrics and make the metrics more specific. Metrics are devised according to a definition of security. As it has been seen, security is multifaceted so defining security for measuring is vital in order to have metrics that will serve the purpose. CIA triad attributed and ARM (availability, reliability and maintainability) are some aspects that could be considered when defining security. Moreover, other specific definitions like number of intrusion, spoofing and sniffing abilities could be the target to find metrics for.

Quantification of security measures is the main area to focus on in security measurement, this is done by having metrics that are obtained from the analysis and comparison of different accumulated data from information system(s). To devise metrics one will need to have or generate these data. Nevertheless, knowing the application of metrics before deriving them will make easier not only to decide on a type of scales or units that will be used but also reporting process.

Many measurements for security are currently qualitative. Although many stakeholders are putting up more efforts in quantifying security measures, the qualitatively measures have shown to be helpful in serving the purpose of measuring and helps the decision making although the precision from metrics would make it even better.

5

SECURITY MEASUREMENT STANDARDS

We now take a look at some commonly adopted industry standards that stakeholders use in order to measure security. Some standards provide guidelines for measuring the security of a system while others take the generic approach by also considering other aspects such as people and organisational management. The selection criteria for the standards reviewed in this section has already been given in section 2.4 of this report.

5.1 Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is a free, open industry standard that can be used for the assessment and communication of the severity of computer system security vulnerabilities. It allows for means to express the main characteristics of a vulnerability and reflect its severity through generation of a numerical score, with this score complemented by a textual representation.

5.1.1 Metrics in CVSS

In order to assess vulnerabilities, CVSS takes into consideration three types of metric categories. They are the Base, Temporal, and Environmental metrics.

They use the base metrics to ascertain those traits of a vulnerability which do not change over time and are independent of the user environment. They are made up of two subsets of metrics, namely: the Exploitability metrics and the impact metrics.

The exploitability metrics are there to give a view of the simplicity as well as technical means by which the vulnerability can be taken advantage of by an attacker. They are said to represent traits of the object that is vulnerable, which in CVSS, is formally referred to as the *vulnerable component.* The Impact metrics, on the other hand, reflect the downright outcome of a successful vulnerability exploit on an object. In terms of CVSS, the impacted object is referred to as the *impacted component*

The Temporal metrics are a set of metrics that ascertain those traits of a vulnerability that may change over a period of time in a given environment.

Finally, CVSS define the Environmental metrics to ascertain the traits of a vulnerability that are of effect and specific to a given user environment.

5.1.2 Measurement Methodology

As already mentioned above, CVSS uses three metric categories in vulnerability assessment. These categories are further divided into subcategories in order to have fine grained measures for analysis.

The Exploitability metrics are composed of the following metric attributes:

1. Attack vector (AV): is an attribute that gives more detail about all possible ways a vulnerability can be exploited. Remote attack possibilities get a higher AV score than local ones.
2. Attack Complexity (AC): is an attribute that defines the necessary state that a vulnerability should have in order for it to be exploited. The AC is not influenced by the attacker in any way.
3. Privileges required (PR): is an attribute that elaborates the privileges required by an attacker before they can successfully take advantage of a vulnerability.
4. User Interaction (UI): is an attribute that weighs in on the role of the user rather than the attacker, in making it possible for a vulnerability to be exploited.

The above metric attributes are used in the derivation of scoring equations as will be explained.

The Impact metrics are composed of the Confidentiality Impact (C), Integrity Impact (I), and Availability Impact (A) metric attributes. These measure to what extent the confidentiality, integrity and availability of information resources of an exploited vulnerability are affected, respectively.

Finally, the Temporal metrics are composed of; the Exploit Code Maturity (E), an attribute that measures the possibility of an attack on a vulnerability by considering present conditions of exploit approaches; the Remediation Level (RL), that puts into consideration prioritization of the vulnerability by taking remedial steps to combat it; the Report Confidence (RC) measures the levels of credibility in the existence of a vulnerability as well as the known technical details associated with it.

5.1.3 Measurement scales and Mathematical Approach

To assign values to Base metrics, a Base equation is derived from two sub-equations: the Exploitability sub score equation (derived from Base Exploitability metrics), and the Impact sub score equation (derived from Base Impact metrics). The Base equation results in a scoring that ranges from 0.0 to 10.0. There are instances when it is necessary to adjust the Base equation by also taking into consideration the Temporal and Environmental metrics so that there is a more accurate reflection of the threats posed by the vulnerability in a particular user's' environment.

CVSS mathematically defines the Base score as,

Roundup(Minimum[(Impact + Exploitability), 10]) provided the scope is unchanged.
And,
Roundup(Minimum[1.08 (Impact + Exploitability), 10]) when the scope is changed.

Here *"Roundup"* is basically the smallest number, reduced to one decimal, that is equal to or higher than its input.

The Impact sub score (ISC) is mathematically defined as,

6.42 x [ISCBase] when the scope is unchanged and,

7.52 x [ISCBase - 0.029] - 3.25 x [ISCBase - 0.02]15 when the scope is changed.

In this case, ISCBase = 1 - [(1 - ImpactConf) x (1 - ImpactInteg) x (1 - ImpactAvail), where the subscripts Conf, Integ and Avail represent the attributes of security.

The Exploitability sub score is mathematically defined as,
8.22 x AttackVector x AttackComplexity x PrivilegeRequired x UserInteraction

The equations of the Temporal and Environmental scores also take a somewhat similar approach in their construction. The metric values of each of the attributes making up these sub scores can be seen in [1]. Interestingly, the standard also has a way of mapping these scores to a qualitative severity rating scale. The scale maps the CVSS scores of the range 0 to 10.0 to ratings ranging from None (0.0), Low (0.1 - 3.9), Medium (4.0 - 6.9), High (7.0 - 8.9) to Critical (9.0 - 10.0) , in increasing order.

It must be noted that CVSS explicitly mention that these formulae provide a mathematical approximation and that the CVSS Special Interest Group (SIG) committee had to assign values to real vulnerabilities. These are the ones that are mapped to the qualitative severity scale described above after the scoring is done. How they came up with these values assigned to various vulnerabilities of the above described metric attributes is not given in the official documentation of the standard. Perhaps suggesting that this was done subjectively.

5.2 ISO/IEC 27004:2009

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are two bodies that are responsible for the formulation of directives that act as a guide for the development of International Standards and related publications. With regard to the development of Information Technology standards, they achieve this through the joint technical committee (ISO/IEC JTC 1) comprised of members from ISO/IEC in liaison with other organizations that share mutual interests.

To provide guidance on the development and use of measures and measurement for the assessment of the effectiveness of an implemented information security management system (ISMS), the ISO/IEC JTC 1 prepared the ISO/IEC 27004 standard. This standard also provides guidelines to assess the effectiveness of controls (or groups of controls).

5.2.1 Measurement Method

ISO/IEC 27004 specifies a measurement model that maps an information need to its related objects of measurement and their identified attributes. Aside from computer systems, the objects of measurement could also include processes, procedures, projects and resources. The standard stipulates that using such a measurement model allows for the quantification of those attributes identified as being applicable to an object of measurement. This indicates that not all attributes of an object may be required in order for measurement to take place, since not all of them might provide useful values depending on the objective of the measurement programme.

Once the object and its attributes have been identified, base measures can be derived by using a measurement method on the attributes of a given object. The base measures are thus said to be the simplest measures that can be obtained. Many base measures can be derived from a single attribute given this approach.

5.2.2 Mathematical Approach

Once base measures have been established and derived they can be used as input for derived measures. Hence, derived measures serve as aggregate measures generated from a set of base measures. ISO/IEC 27004 defines a measurement function as being the calculation that makes it possible to combine two or more base measures in order to come up with derived measures. E.g calculating average values using base measures or assigning qualitative values to base measures could be considered as measurement functions applied to base measures.

For the derived measures described in the paragraph above, the scale and unit used is always dependant on the base measures used in the derivation as well as on how they are aggregated in the measurement function.

As a way of getting more information out of base and derived measures, the standard defines indicators. An indicator is basically a measure that estimates or evaluates selected attributes with the aid of an analytical model. Indicators are used for the interpretation of values assigned to measures in line with set decision criteria and/or information needs of stakeholders.

The design of the analytical model is done with the information needs of stakeholders acting as a guide. However, the decision on which analytical methods to use for the generation of indicators is dependant on the scale and measurement method used.

5.3 Common Criteria

5.3.1 Introduction

Common Criteria, abbreviated and referred to as CC, is an international standard developed for the certification of computer security and is defined in ISO/IEC 15408. It allows for computer system users to describe their security requirements through the use of Protection Profiles (PPs). Common criteria also allows vendors to implement security attributes of their products and also to make statements about that security. CC also gives evaluators and testers a guiding framework to use in order to evaluate IT products and validate their security claims.

The CC takes an active approach in determining whether a particular IT product meets its security objective by carrying out an investigative evaluation of the product. The result(s) of such an evaluation is called an *Assurance*.

To measure security assurance, the CC makes use of the concepts of Target of Evaluation (ToE), Security Target (ST), Protection Profile (PP), and Evaluation Assurance Levels (EAL), among others.

A *Target of Evaluation* (ToE) is the system or product whose security assurance is to be evaluated.
A *Protection Profile* (PP) is specified by system users and/or a user community in order to provide an implementation independent specification of security requirements. These security requirements include functional and assurance levels, SFR and SAR, respectively. It is crucial that the PP specifies the threats, objectives, and security requirements in order for an evaluation to accurately verify and validate claims made by a vendor of a given system.

CC also specifies the *Security Target* (ST). ST defines the security requirements of a ToE and has implementation-specific information showing how the ToE meets these requirements. The ST may fulfil some or all of the requirements specified in the PP of a given system.

Once an evaluation is completed, CC assigns a *Evaluation Assurance Level* (EAL) to the product that was being evaluated. The EAL is a numerical grade that, rather than reflecting the security of the product evaluated, reflects to what level the product was tested with regard to CC. CC specifies a range from EAL1 to EAL7, with increasing assurance levels reflecting added assurance requirements that must be met to achieve Common Criteria certification.

The figure 3.3 shows the relation of how the above explained principles ultimately end up into the evaluation of a system.

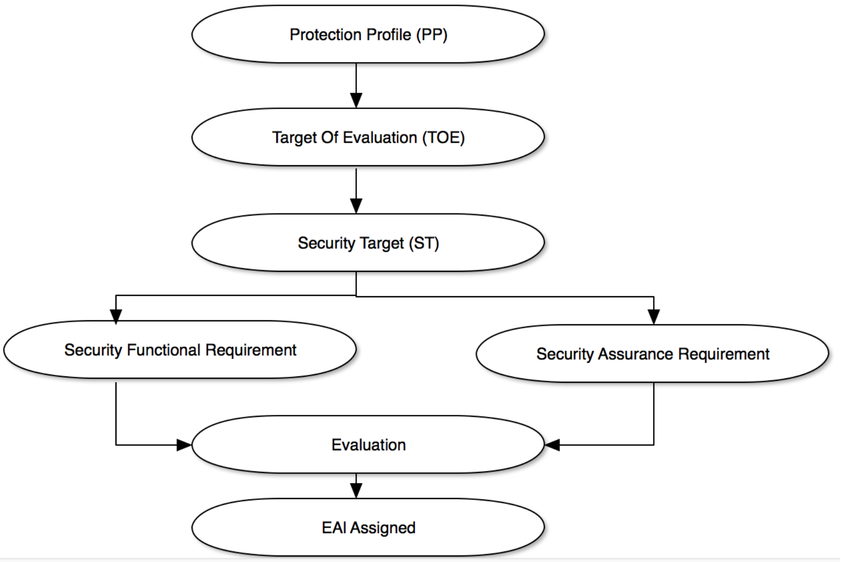

Protection Profile (PP)
Target Of Evaluation (TOE)
Security Target (ST)
Security Functional Requirement
Security Assurance Requirement
Evaluation
EAl Assigned

Figure 5.1: Evaluation of a system according to Common Criteria

5.3.2 System Model

The Common Criteria takes a generic approach towards modelling of the ToE with regard to security considerations. The ToE could be anything from software, hardware, or a network, to information that is processed, stored and transmitted. The owners and/or persons with interests in the ToE may seek to preserve its confidentiality, integrity and availability by having means of identifying possible threats and the threat origins (hereby known as threat agents in CC terminology).

Threat origins may include hackers, bad system design, viruses, malware, and bad system administration, among others. An introduction of threats to a ToE has the potential to impair its normal state thereby reducing its value. Therefore, it is imperative that threats are identified in order to ascertain the related risks associated with them. Once this is accomplished, necessary steps and points of action can be formulated and aggregated into a set of countermeasures.

The level to which the CIA attributes of a ToE are preserved is determined by how much value the system owners place in the asset (ToE).

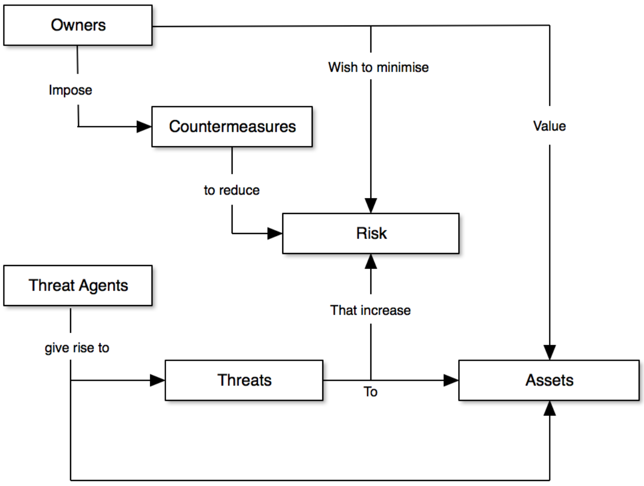


Figure 5.2: System modelling for security measurement in CC

5.3.3 Measurement Method

The CC takes a different approach in its measurement methodology as compared to most security measurement standards in the sense that it emphasizes that greater assurance is achieved by putting more effort in the evaluation process. As stated already, CC specifies seven assurance levels with increasing level of assurance with each increasing level.

5.4 Summary of Security Measurement Standards

A look at the standards shows that regardless of the methodology or approach employed, the goals and objectives of the measurement programme are critical in influencing the metrication steps. Well defined objectives assist in coming up with a clear road-map towards metrication. The road-map is key in specifying steps to be taken during the measurement and, these steps aid in the design of metrics to be used in the metrication process as has already been mentioned in previous chapters.

The standards analysed also emphasized the need for continuously carrying out metrication due to the dynamic nature of security. Security considerations are always changing hence this places a requirement to always revise the set objectives of the measurement programme and re-align the metrics design process to the new requirements. The extent of the security considerations is, of course, dependant on how much value is placed on the system and/or environment whose security is being measured.

6
INTERVIEWS

6.1 Introduction

We now present important points to note from interviews conducted with a few companies. The companies range from medium to large sized companies where a company with between 30 and 100 employees is considered to be medium sized and one with over 100 employees is considered to be a large company.
The interviews were semi-formal, guided by some pre-set questions shared with the interviewed participants prior to the interviews. The set of questions and the motive behind every question can be found in Appendix 1. These questions served as a guide to the discussion but other questions were introduced along the discussion.

The companies targeted for this activity were of different sizes ranging from medium to large companies including security consultancy firms, automotive companies and institutions offering banking and financial services to the public. The security consultancy companies were targeted because they offer consultancy services to clients from various industry backgrounds hence their insight was all encompassing. Automotive companies were considered because they are today incorporating computer systems in their products and this comes with its own security considerations. Banking and financial services institutions were also considered because, according to Interpol, they together with their customers, are one of the major targets of cyber criminals hence knowing how they manage and measure security was of profound interest to our project.

6.2 Ethics and Anonymity

Throughout this section we do not disclose the names of the participants nor the names of the organisations they were representing at the time of interview. We shall instead identify the participants as interviewee 1, 2, 3 and each company as company A, B, C etc. The information gathered from these interviews is deemed to be the most important facet from the interviews for the purposes of this thesis.

Other company specific details such as Security policies and procedures as well as other business sensitive information will not be discussed in this section. Rather, the focus will be on the details of measurement approaches and methodologies employed in measuring of security. This information may also be confidential information of the involved companies hence we made sure to inform the participants that they would only discuss details up to a point deemed not to be confidential. This means all the information in this section was considered not to be private and confidential during this activity.

6.3 Interview 1

6.3.1 The Companies (A and B)

The participant in this interview shared their experiences based on their roles in their previous place of employment (herewith called company A) and their current place of work (herewith called company B).

Company A is classified as a large company in the telecommunications industry. It offers telephone, cable and Internet services for domestic, commercial and mobile customers. The focus of information security in this company is for internal operational, risk and financial purposes. More details with regard to this are given below.

Company B is classified as a medium sized company in the IT consultancy industry. Its business objective is to deliver a full-suite of IT services and solutions to other organizations, security consultancy services being one of them. Our focus was to find out how exactly they carry out the security measurement with regard to methodology and approach, and whether the results are qualitative or quantitative.

6.3.2 Role of Interviewee: Security Consultant

Company A:

Question: Do you use any metrics in measuring security?

Interpretation of interviewees answer to the question
According to the interviewee, Company A used a set of metrics in terms of scores for the measurement of security. The scores used were numerical values ranging from 0 - 3, where 0 was low and 3 was catastrophic. Although the same was being done to both non information and information related systems but for the purpose of our work we only focused on information systems. The scores were given according to monetary cost impact they had on the organization. For example, a breach in the network that would cause the entire system to go down was considered to be catastrophic or any incident that would cause a loss of say one billion SEK, would be considered to be catastrophic. Other repercussions like loss of human life also fell in this category.

Our interest was to know how these scores were arrived at. It was revealed that all these scores were obtained subjectively by the analyst who is near omniscient about the system under measurement. The fact that the scores are arrived at in a subjective manner gives rise to the possibility of having different scores on the same systems if the measurement is done by two different people. Also, the metrics were being changed regularly to fit the purpose of measurement but still they were not quantitative.

Company B:

Refer to Questions 4 to 11 in appendix A.

Interpretation of interviewees answers to questions 4 to 11

The security consultants in company B mostly use the Centre for Internet Security's 20 critical security controls (CIS CSC) in order to carry out security assessments. The CIS CSC define 20 different areas of possible security incidents and breaches [5] and how to circumvent them. A full-stack assessment involves assessing all the critical controls while other assessments only focus on a single control or a combination of some controls. Which critical security control to assess is always dependant on the measurement programme and its objectives.

The possible affected entities (systems, IT products, etc) are outlined and evaluated according to the required controls as determined from the set objectives. Scores from 0 - 3 are then given to every entity according to the defined scoring convention as depicted in table 6.1.

An example is shown in the figure below of a case where only 3 critical security controls are under assessment. Each Critical Security Control (CSC) is given a score ranging from 0 to 3 where, 0 means not applicable, 1 is low, 2 is medium and 3 is high with regard to severity. The total value of a CSC is obtained by taking the average of the scores across the parameters being considered. For example in an assessment of a virtualized server system, the system might be composed of parameters 1, 2, 3 (windows OS, a Linux distribution and Unix OS in this case). The separate scores for each machine (parameter) with regard to a security control, e.g. malware protection, is summed up and the average is computed to give an overall score of that control. Table 6.1 shows that Mac OS, Linux and Unix have scores of 1, 2 and 3 for the malware protection security control respectively, hence giving an average overall system reading of 1.5 for this control.

Table 6.1: Ranking the Critical Security Controls

Security Control	Par 1 (e.g MacOS)	Par 2 (e.g Linux)	Par 3 (e.g Unix)	Average
Malware Defences	1	2	3	1.5
Penetration Tests	3	3	3	3
Data Protection	2	2	2	2
Average	2	2.3	2.7	2.2

KEY:
0 : Not applicable
1 : Applicable but not adhere to processes and procedures.
2 : Adhering to but not documenting.
3 : adhering to and documenting.

The scores are given by the analyst in a subjective manner guided by a scoring system. This goes to show that the task of measuring security seems to be non-trivial and to heavily rely on the competence of the consultant and his/her expertise on the subject.

As depicted in the figure above, the total scores of a given CSC on an entity comprising different sub-components (parameter 1, 2, 3 etc) can be obtained by summing up the total scores horizontally to give the score of a control in that entity. It is sometimes necessary to know how each sub-component (parameter) is performing with respect to all the security controls under assessment. This is achieved by taking the average score of the parameter vertically thereby obtaining the security posture of the parameter with regard to the security controls under assessment.

It can be observed that merely calculating average scores might not give an accurate reflection of the security controls under assessment, especially for a composite system . Consider a case when the overall score of a given CSC seems to be a reasonable value say 1.5 which might seem to be fair (medium severity) but one of the constituting parameters had say 3, which has high severity. It is better in such a case to take note of all outliers used in the calculation of the average values so that a clear picture of the real security posture is seen. How the outlier values are treated is dependant on the objectives of the assessment, as has already been said.

6.4 Interview 2

6.4.1 The company (C)

The company (herewith called company C) is a large company that offers banking and financial services to its customers. They host a number of electronic banking services such as mobile banking, the core banking system, internet banking, card management systems, among others. A large part of these IT services are hosted internally with only a few of them outsourced. It is crucial to offer these services to their customers in the most secure ways possible in order to avoid any financial, operational, reputations and other types of risks.

This interview with company C was conducted by phone and the main focus was around the security measurement methodologies and approaches the company uses in order to meet its security objectives. Company C is ISO/IEC 27001 certified and adheres to all the information security management procedures specified in the standard. The main objective for the company getting certified according to this standard was to ***minimize the number of incidents*** in information systems and processes.

6.4.2 Role of interviewee: Security Manager

Question: How do you measure security with consideration of some factors below?

- System modelling
- How you define security
- Measurement methodology

Interpretation of interviewees answers to the question
They do not have a pre-designed security model to guide doing the process. The work is done through penetration tests and other tools to gather information related to set objectives (e.g. trying to get the number of possible incidents in a system). OpenVAS and Nessus are among the tools used to get information on the security levels of systems under investigation. The use of LOW, MEDIUM, HIGH ratings as suggested by OpenVAS manual [reference to manual here] is taken into consideration when it comes to decision making and mitigation of the same. There are times when business requirements and/or the importance of the system under assessment calls for stringent action even though the scores from the vulnerability tests revealed otherwise.

The measurements are done by an IT security team and are used by them to know the security posture of the systems used in the company. The measurements are also used by the risk department to determine if there is associated risk with other ongoing activities. The risk and IT security teams both have the relative metrics for comparison with what had been found previously.

Measurement is done by considering the subsystems constituting a system/IT product. For example if the there is a web-server with MySql database and Linux system, then both are measured separately to get the insight on their security status. The idea is good when it comes to mitigation/prevention and detection, though having a score/overall rating on the entire system could be helpful in decision making.

All the scores on measures where subjective which suggests that the person conducting the tests and doing the ratings in order to form a metric must be knowledgeable in the field.

From the interview, we can summarize the findings as follows:

1. The first thing the company does is to set the objective
2. The scores and ratings are subjective
3. The type of metrics used are relative and qualitative
4. The metrics are mostly used to improve security of the systems
5. The measurement is done on sub-systems in the case of composite systems.

6.5 Interview 3

6.5.1 The Company (D)

The company (herewith called company D) is a large company in the automotive truck industry involved with technology research and product design and development. The company is also responsible for product support during the after sale period. Current research is aimed towards coming up with automotive trucks that have connectivity and related computer systems embedded in them. The connectivity allows for truck-to-truck communication as well as communication to other external networks such as the Internet.

The ability to embed connectivity in the automotive products has also spearheaded research into self-driven trucks. However, with this advent of features comes security considerations of critical importance to the core attributes of security (i.e. the CIA attributes). Security considerations are also of far-reaching importance when you consider how they relate to the safety of the automotive products given such possibilities.

6.5.2 Role of interviewee: Technology Specialist

Question: How do you define security (e.g minimizing risks, viruses, vulnerabilities etc) and
Question: Do you use any metrics in measuring security? If yes, are the metrics derived by you/your company or are guided by a security measurement standard?

Interpretation of interviewees answers to the questions: Company D have developed their own threat centric framework of guidelines, called HEAVENS D2, to be used when measuring security. The company also makes use of the OCTAVE security measurement standard [52] alongside HEAVENS D2.

HEAVENS, which stands for **HEA**ling **V**ulnerabilities to **E**nhance **S**oftware **S**ecurity

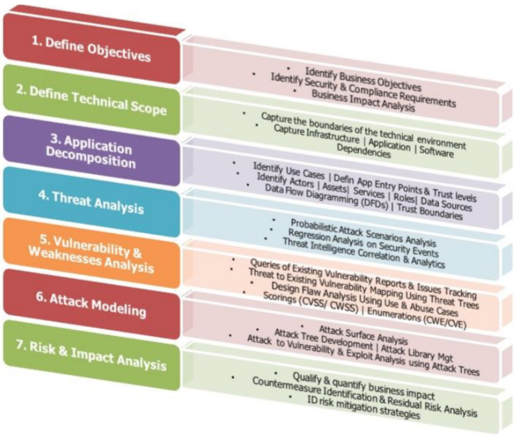

1. Define Objectives
Identify Business Objectives
Identify Security & Compliance Requirements
Business Impact Analysis
2. Define Technical Scope
Capture the boundaries of the technical environment
Capture Infrastructure | Application | Software Dependencies
3. Application Decomposition
Identify Use Cases | Defin App Entry Points & Trust levels
Identify Actors | Assets| Services | Roles| Data Sources
Data Flow Diagramming (DFDs) | Trust Boundaries
4. Threat Analysis
Probabilistic Attack Scenarios Analysis
Regression Analysis on Security Events
Threat Intelligence Correlation & Analytics
5. Vulnerability & Weaknesses Analysis
Queries of Existing Vulnerability Reports & Issues Tracking
Threat to Existing Vulnerability Mapping Using Threat Trees
Design Flaw Analysis Using Use & Abuse Cases
Scorings (CVSS/ CWSS) | Enumerations (CWE/CVE)
6. Attack Modeling
Attack Surface Analysis
Attack Tree Development | Attack Library Mgt
Attack to Vulnerability & Exploit Analysis using Attack Trees
7. Risk & Impact Analysis
Qualify & quantify business impact
Countermeasure Identification & Residual Risk Analysis
ID risk mitigation strategies

Figure 6.1: P.A.S.T.A. model of threat and risk analysis

and Safety is a project that was conducted by Company D between April 2013 and March 2016. The aim of the project was to present the state-of-the-art threat analysis and risk assessment methodologies, processes, frameworks and tools by considering industrial IT security, telecommunications and software engineering. Later, the project established a HEAVENS security model for the automotive industry based on the presented methodologies.

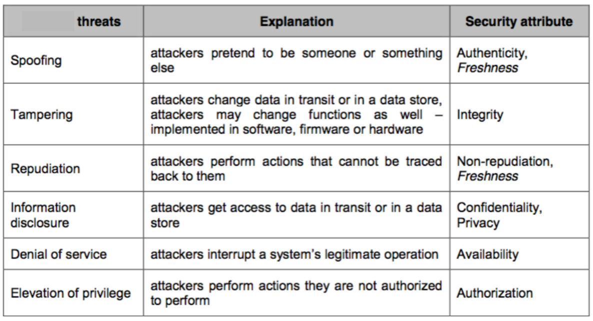
The objectives set for the HEAVENS project were adopted from **OWASP** concepts and included but were not limited to Identity, Financial, Reputation, Privacy and Regulatory and Availability objectives. Other impacts like laws, Regulations, Standards, Legal agreements, corporate Information Security etc. Other considered objectives in this project were taken from the **EVITA** project[41] which included safety (of vehicle occupants and other road users and infrastructure), Financial (prevent negative financial impact), Operational (maintaining the intended operational performance of all vehicles), among others. The security modeling involved the three steps:-

1. i. Characterizing the systems;
2. ii. Identifying assets and access points;
3. iii. Identifying threats.

Different models contributed towards the formation of HEAVENS including; Microsoft **STRIDE** and **DREAD** [45] and **PASTA** (Process for Attack Simulation and Threat Analysis) which shows how threats are analysed with the objective of minimising risks associated with the business. The model comprises of different stages as shown in the figure below:

Question: which security aspects are covered (by considering CIA or other dependability factors)

Interpretation of interviewees answers to the question



threats	Explanation	Security attribute
Spoofing	attackers pretend to be someone or something else	Authenticity, *Freshness*
Tampering	attackers change data in transit or in a data store, attackers may change functions as well – implemented in software, firmware or hardware	Integrity
Repudiation	attackers perform actions that cannot be traced back to them	Non-repudiation, *Freshness*
Information disclosure	attackers get access to data in transit or in a data store	Confidentiality, Privacy
Denial of service	attackers interrupt a system's legitimate operation	Availability
Elevation of privilege	attackers perform actions they are not authorized to perform	Authorization

Figure 6.2: A diagram Figure showing the mapping between threats and security attributes.

The HEAVENS model starts out by defining a security model which acts as a means for simplifying the design of a system and defining security. The main security attributes (CIA) were supplemented with privacy, authenticity and trustworthiness, non-repudiation, accountability and auditability according to the OCTAVE standard [55].

Question: How do you define security (e.g minimizing risks, viruses, vulnerabilities etc)

Interpretation of interviewees answers to the question
The objective of measuring security for the company was to reduce risks. Setting Objectives is company dependent, i.e depends on the business type and priority of the company. For example a bank and a car company might have different concepts with regard to security. A bank might concentrate on the monetary losses that might happen while a car company might concentrate on the life risks or environmental risks. This company took risks as the main objective that might be caused by both dependability (ARM) and security (CIA) factors.

The development of HEAVENS threat centric model adopted the concepts from Microsoft's STRIDE approach with regard to automotive E/E (electrical and electronics) systems. It also establishes a direct relationship between the threats and the affected security attribute(s) during a threat analysis as shown in figure 6.2. This makes the estimation of impact on an asset due to violation of a certain security attribute. The main objective of HEAVEN is to assess risk and analyse threats with a limitation of inability to establish a relationship between vulnerabilities and threats.

Question: How do you do System modelling during security measuring?

Interpretation of interviewees answers to the question
The company uses data flow diagrams and other methods (not specified in the interview) to get the overview and possible threats against the TOE (Target of Evaluation) in terms of security breaches. This is an upswing concept that we believe it

could help and make the process of measuring a bit easier. Identifying the type of system to be measured gives a cruel on different aspects of security that an analyst should base on, the company has defined two systems that they work on, a network and software system.

Question: What measurement methodology do you use?

Interpretation of interviewees answers to the question
A top-down methodology was identified as a primary method used to derive metrics and scores/ratings. The different attributes may arise depending on the various contingencies. This is because one or more security/dependability attributes failure may result into another failure in another security/dependability attribute. The company marks death as a critical risk followed by monetary factors due to indemnification events or something else related to that. Other detailed ratings criteria can be found in HEAVENS D2.

From the discussion and input of the interviewee, the findings are summarized below:

1. The objective of measuring risk is to reduce risks
2. The company uses scores and levels of severity to measure different incidents
3. The scores are subjectively assigned to different incident levels or findings
4. They take advantage of threat security modelling to identify possible threats
5. Attributes apart from the triad (CIA) are used
6. Every possible threat iss mapped to the impact it causes to the security attributes
7. They consider the effect of one attribute to another attribute to measure security (for example the stolen car can result into sustainability effects)
8. They adopted metrics based on OCTAVE in HEAVENS framework
9. The metrics used are qualitative and mathematical values are derived subjectively.

6.6 Interview 4

6.6.1 The Company (E)

Company E is a large company that is one of the leading global car producers. They produce cars ranging from sedans to SUVs and are also involved in offering after sale services for these cars. The company is currently involved in a lot of research and development in the area of self-driven and networked cars, and they see this as the technology of the future for vehicles.

As with Company D in the previous interview, having such connectivity features and their related computer systems incorporated into cars brings about the possibility of security vulnerabilities. Therefore there is need to make security assessments and considerations in the process of introducing such features in cars. The company uses the ISO/IEC 27000 series of standards as a guide to how they manage the information security of their products.

6.6.2 Role of interviewee: Designer (Electrical Systems, RD)

Question: How do you define security (e.g minimizing risks, viruses, vulnerabilities etc)?
Security of the systems on the cars is defined in terms of risk. The main approach is to identify the subsystems that are security relevant in the car and then carry out an assessment of whether there are any risks present or not with respect to security. The key focus is risk minimisation in the subsystems and this is achieved through threat modelling by considering the various commands and data elements that are present in the subsystems. The commands and data elements are analyzed by looking at how they affect the security attributes of the CIA triad.
Question: What measurement scales and scores do you use in the measurement exercise?
The company uses the conventional common vulnerabilities and exposures (CVE) scoring system of low, medium and high in terms of representing the severity of identified risks within a subsystem. To arrive at a particular score for a risk, engineers and other stakeholders are consulted and the scoring ends up being subjective, based on an engineering judgment. However, the classification of the risk level is not the key focus but rather the mitigation of the identified risk(s) then becomes the focus of attention. This entails that when a risk is identified, mitigation steps are formulated and necessary steps taken to minimize or get rid of the risk. Thereafter, rigorous testing including positive and negative system tests are carried out.
Positive testing involves validating the system using valid input data with the intention of finding out whether an application behaves as expected when supplied with its expected input. This testing is used to show that a given system or product meets its set requirements and specifications. Negative testing on the other hand involves validating a given system against invalid input data by checking that the system behaves as expected when supplied with negative input i.e. with unexpected input data. This type of testing thus tries to show that a given system or product is stable even in the presence of invalid input data sets.
Because of the criticality of the safety of the cars Company E makes, they try not to focus much on scoring the risks but rather on getting rid of the risks through the setting up of relevant controls and thorough tests to ensure the risk is mitigated.
Question: Are there any mathematical approaches used during the measurement exercise?
The CVSS mathematical approach explained in section 5.1 of this report is also adopted by company E. However, they only use the approach at a subsystem vulnerability level i.e. when assessing and measuring the security of software components within the subsystems of the car. The results of this assessment are then aggregated and their risk level translated into monetary value at a higher business level. The monetary value is arrived at by considering how the risk would affect finance, legal, environmental and other aspects if not dealt with. Question: What are the application areas of your measurement results?

The sole purpose of the measurement exercise is to discover and identify risks in computer systems within cars and then mitigate these risks. The results of these steps are then communicated to management with enough interpretation of the details of every step carried out and also advice as to whether the product assessed is for the market or not.

Apart from communicating the results to management, the results are also used for comparison purposes. An external consultant is brought in to carry out tests in order to have second (fresh opinion) of the risk position of systems within the cars. The consultant takes the approach of white box testing where the subsystems are tested at source code level by considering the design techniques adopted in the development of the subsystems rather than concentrating on their functionality. The results of the external consultant are later compared with the ones obtained by the internal security team of the company and necessary improvements are made if required.

Important points of note from the interview in summary include:

1. Top-down approach used in initial risk analysis exercise
2. However, verification and validation is done using a bottom-up approach

6.7 Summary

The conducted interviews gave a fair reflection of how industry approaches the measurement of security. Generally, it can be seen that industry is influenced by the commonly adopted security measurement standards. These help in guiding the measurement process as well as the risk modelling process, in cases where risk modelling is chosen as a means of measuring security.

It can also be seen that there are times when industry formulate their own metrics and measurement approaches in order to meet the set objectives of the measurement programme. Nevertheless, these are heavily influenced by the widely adapted security measurement standards.

7

A SUGGESTED POSSIBLE MEASUREMENT PROCESS FOR SECURITY

7.1 Introduction

After having reviewed how research, the standards and industry handle security measurement, we identified a need for having pragmatic steps to guide companies and organisations in the process of measuring security. This section presents our suggested steps that can be used as a guideline when measuring the security of a system. It is a hybrid model that comprises of 9 steps that have been developed based on practices from various sources such as standards surveyed, research work reviews and from personnel in the companies interviewed. We found these practices to be sound and fit in the development of this model.

Our suggested process looks at measuring security by considering security as a feature/property incorporated in a system. Thus the measurements and metrics aim to find out and communicate to what extent a system is secure (i.e ensuring that the identified security attributes are not compromised). This notion of security is adopted from [35], where it is stated that security can either be viewed as a state of an organization or a property of a given system.

Each step in the model, the design criteria and the approach(es) were inferred from the study and survey of standards, research and industry.

7.2 Steps in Measuring Security and Metrication

The proposed process has eight steps that can guide the measuring of security and metrics formulation. The following subsections explain each step in the process. It should be noted that the process uses the top-down approach (already explained in previous sections) towards measuring security as well as for metrics derivation.

7.2.1 Step 1: Objectives

What is the objective of the Measurement Activity?
Measurements and metrics formulation are carried out for many reasons. A mea-

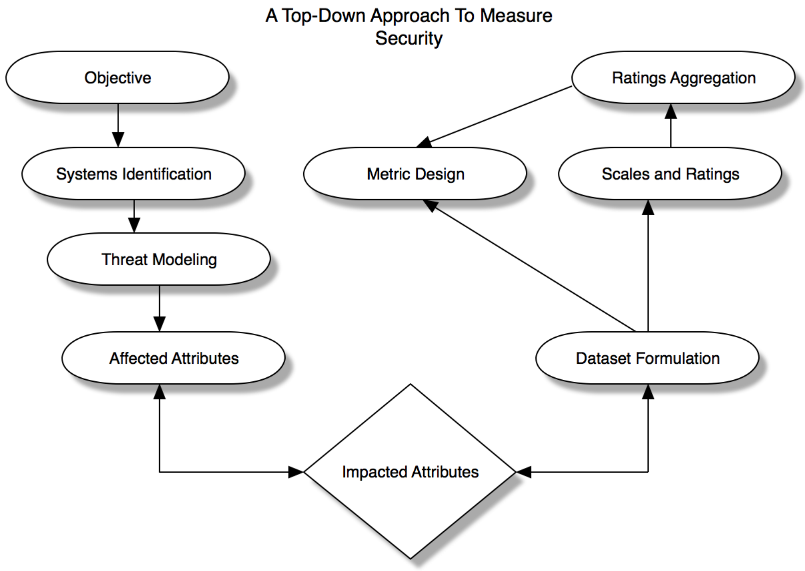


Figure 7.1: A hybrid model to measure security-Top down approach.

surement activity must therefore be embarked on with stipulated objectives set beforehand in order to have clear steps to be undertaken for its success.

The International Organisation for Standardization and International elctrotechnical comission (ISO/IEC) 2009 [37] mentioned some factors that are useful in the inception of measurements objectives as follows:

1. Effectiveness of policies, processes and procedures.
2. Legal, contractual and Regulatory requirements and obligations.
3. Decision making.
4. The return on investment of the measurement activity.
5. The criteria used to accept Risk by the system owner.
6. Comparisons with other measurement activities.

Other objectives could also be included to this list depending on their applicability to the measurement activity and expectations from the outcome. From most of the literature we have reviewed so far [24, 25**?** , 5, 30], setting objectives seems to be an important step before metrics derivation. Objectives can also be used to assess and verify the entire process in whether it has achieved the desired purpose or not. As we have chosen to adopt the top-down approach, objectives setting is the crucial step towards security measurement and metrics formulation. The GQM approach described in section 4.2 also supports this notion. After measurements have been done, the process can work backward to a bottom-up manner in order to verify and validate whether the objectives are met or not. Measures can then be used to form metrics.

7.2.2 Step 2: Systems Identification

Once the measurement objectives have been identified and documented, it is necessary to identify the system or subsystems constituting the system whose security is to be measured. Is it a single component system or a composite system? This is a fundamental question to be addressed when measuring security. For this purpose, we conform this step to the approach taken by the Common Criteria (CC) in identifying aspects to be measured and the whole concept to come up with measurement of each subsystem. Other methods could also be used. This process will help identification of common vulnerabilities in some known systems like network, software, cloud systems and MANETs, among others. It also helps in designing the threat model for threat identification.
The concept of a Target of Evaluation has already been explained in section 5.3 of this report, and CC state that a ToE can be anything from software, firmware, and/or hardware. The ToE could be an IT product, a part of an IT product, a combination of IT products or a unique technology that may never be made into a IT product, or some combination of these. CC guidelines are therefore more suited for the systems identification step since they have a clearly defined criteria for setting the system boundary in order to enable security measurement.

7.2.3 Step 3: Threat modelling

At this point the objectives of the security measurement have been set and the system boundaries of what has to be measured has been set. The next step is to carry an analysis of the possible threats to the security of the system under measurement and this can be achieved through threat modelling. A threat model gives an abstract view of possible threats and risks that a system is exposed to. As suggested by Microsoft [43], a threat model helps to identify and analyse different risks on a system. The model can also help designers identify and predict the capability of an attacker [36]. A lot of security threat models have been suggested like Microsoft's STRIDE, etc. In this work we will consider the overview of Microsoft security modeling concepts and its fundamental steps in developing a threat model. We will also consider the threat model in [13] because it has considered both input and output behaviour of a system when subjected to various environmental threats.

Threat modelling helps identifying the security assumptions considered for a system and reflects the confidence of how much a system is secure and its limits. Threat models also help with the specification of security requirements in a system and their bases. In the security engineering process, threat modelling presents the possibility of exposing possible threats to a system regardless of whether they are exploitable or not. This involves identifying the type of system, type of expected users and where the system is used and consider countermeasures to reduce the risk of in case of vulnerability exploitation. Having a threat model also helps the process of measuring security and metrication by identifying security attributes which are key points in the process. Myagmar [36] shows how a threat model can be useful in the security engineering mechanism as shown in a figure 7.2 which has a cycle design where each stage can feed other preceding phases (stages) for review and rectification. Our

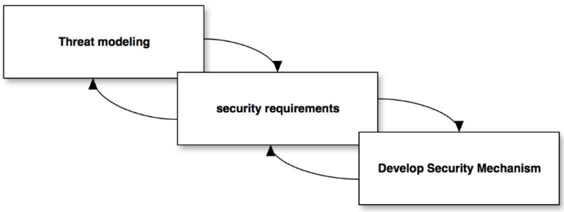


Figure 7.2: Security engineering mechanism

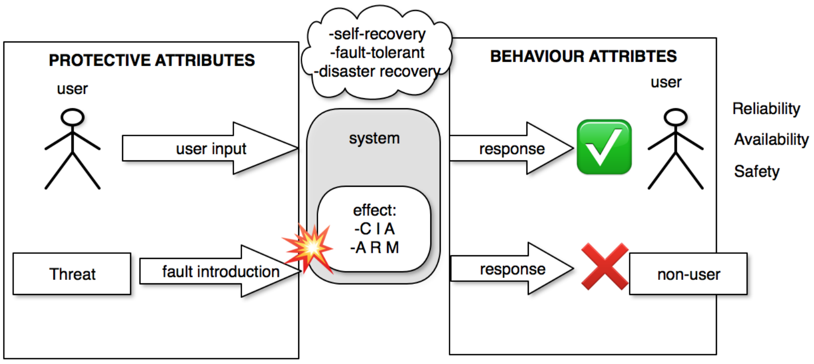


Figure 7.3: A figure showing dependability and security attributes behaviour

suggested model will consider both security and dependability factors affecting the system as explained in section 3.2. These factors that might affect a system are shown in figure 7.2:

As depicted in figure 7.3, the input threat(s) to and output from the system can be described by protective and behaviour attributes. Behaviour attributes show how the system behaves after threat introduction. The system's behaviour after an input may include how the system maintains its reliability, availability, confidentiality and safety when its integrity is disturbed or disrupted.

The model also shows the property of a system with regard to fault tolerance, maintainability and self recovery ability which can be achieved by having backups, disaster recovery e.t.c. To maintain confidentiality, a system must respond to only legitimate users and deny service to non-users. The idea of this model is to identify different possible threats like repudiation, tampering, spoofing, denial of service, information disclosure or privilege elevation according to Microsoft's STRIDE among other possible threats.

7.2.4 Step 4: Affected attributes

Using a threat model as suggested above can assist in identification of possible threats to the system. Once the threats are identified, the corresponding affected security or dependability attributes can also be identified, measured and rated for further analysis and metric formulation according to the set objectives.

Identification of affected attribute(s) may include pointing out the primarily affected attribute (CIA and ARM) and/or other attributes that might have an impact on the previously affected attribute(s). For example, a system might have its reliability attribute affected but in turn this results into a related availability problem as shown in 3.1. Therefore, the process should be able to point out this for further inclusion in measuring security as explained later in the aggregation and scaling steps.

7.2.5 Step 5: Impacted Attributes

The idea of considering how one affected attribute has an effect on another attribute was motivated by interview 3 conducted at Company D. Company D considered the safety of a vehicle in relation to implications on the safety of the car. When some wrong readings are taken as a result of a security breach then another functionality of the car might be affected as well. In cases of connected cars, the breach might affect the security attributes of the other cars with which it is connected to. It is therefore of utmost importance to understand not only the threats to the attributes under observation but also to how their compromise affects other attributes within a given system or in a related system.
This step is also motivated by the CVSS standard as discussed in section 5.1. CVSS considers environmental, temporal and/or human behaviour metrics when analysing the security of the component under measurement.

7.2.6 Step 6: Dataset Formulation

The next step is to find suitable approaches and methods to derive measures and assign values to these measures. This is done by initially identifying measures of the system under measurement and then later identifying various methods for collecting input data to assign to the measures. One approach would be to consider the methods proposed by the SANS 20 Critical Security Controls (CSC) on how to assign values to identified measures. This has been discussed in interview 1 in the interviews section of this report.

Other sources of data could include penetration tests, security logs, risk assessment results, patch management systems, incident reports, external audit reports, questionnaire and personal interviews, to mention but a few. As already mentioned in this report, such steps are guided by the objectives of the measurement programme. This is important because it ensures that the collected measures are a reflection of the security status of the system thus, can be used to come up with appropriate actions for improvement.

Depending on the objectives of the measurement programme, policies and procedures can also be used for data formulation. This relates back to keeping logs and incident reports pertaining to the adherence of the policies and procedures.
The objectives of the measurement programme as well as the implementation plan act as the main guide for data formulation.

7.2.7 Step 7: Scales and Ratings

Assigning scales for measurement should take into consideration both objectives of metrics/measures and the way of reporting results to necessary stakeholders. When choosing scales and units to use, the *plausibility* and *accuracy* properties defined in section 4.4.2 should be considered among other factors. Different scale types were mentioned in the same section.

Qualitative and quantitative approaches could both be used to obtain metrics. If ratings are used (which seems to be the norm as exemplified in CVSS), there has to be a clear definition of what the rating ranges represent. For example using the CVSS convention; medium or average represents a medium severity; low to represent absence or no severity; and high to represent high severity. These should be well documented for further reference especially when determining the overall security of a system comprising of many subsystems having different attributes. The CVSS documentation on how the ratings and scoring are done is a good example for this purpose.

7.2.8 Step 8: Ratings Aggregation (optional)

The ratings aggregation step was considered based on the interview conducted with Companies A and B. The interviewee did emphasize that though the process of ratings aggregation has its own complexities, it still retains some simple aggregation methods which can fairly reflect the security status of a given object(s) under measurement. This step may therefore not be applicable in all instances of measuring the security of systems.

Nevertheless, this step is important in situations where a system has the following properties:

1. The system has more than one component (application, software, process etc) that are interesting for security measurement and an overall measurement for all components has to be determined.
2. The system has only one component but this component has more than one attribute of security to be measured.
3. The system has the combination of the above properties and an overall measure has to be deduced.

If the first property holds, then each component has to be measured separately, e.g. C1, C2 and C3, in figure 7.4. The score/value obtained should comply with a level of severity in a system (i.e low, medium or large if this scale was used). Depending on the objectives and purpose of measurement, the component should be tagged with its score if it has exceeded a threshold value of severity in order to trigger an alarm when the overall average score is deduced. This is useful when the overall score seems fair yet one of the component(s) has exceeded the threshold. Doing so will give a clear picture of the severity at component level to anyone who interprets the resultant measures of the components with higher severity level.

Computer systems usually have one component which has more than one attribute

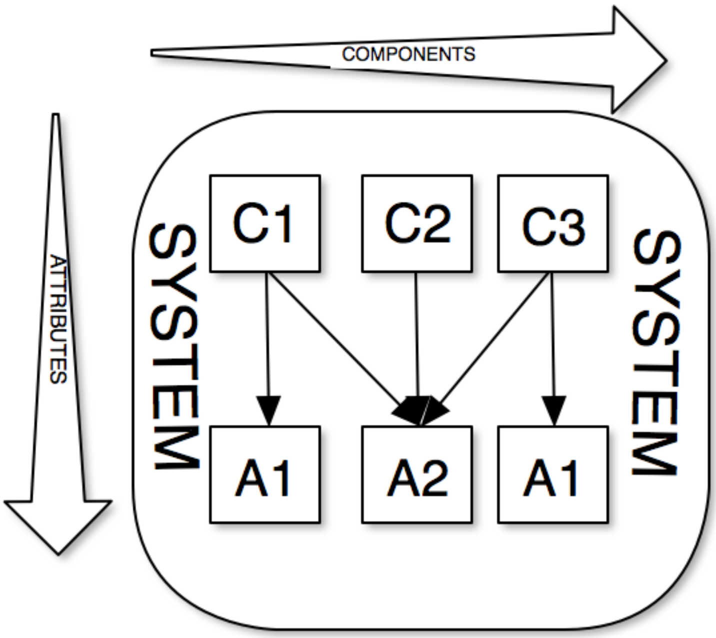


Figure 7.4: A system comprised of sub-components and various attributes

prone to vulnerabilities. For example in figure 7.4, component C1 has two attributes A1 and A2, thus aggregating and averaging all the scores on its attributes might give a final score which is not reflective of the actual security state and may have implications. As described in the previous property, the same could be adopted here in order to give a clear picture on the final score/measure.

The last possible property is the combination of the above properties. As depicted in figure 7.4, the overall score of a component with its considered attributes holding the second property is obtained for each component and then the average score after combining different components is obtained according to property one. The tags for triggering an alarm are all maintained.

7.2.9 Step 9: Metrics Design

Finally, having gone through the steps above, the last suggested step in the measurement process is that of metrics design. As shown in figure 7.3, the step involves comparison and analysis of measurements. In the figure, the process takes values from the data-set which is obtained from network scans, audit results and IDS/IPS data, among others, as described in the subsection 7.9. These data can give an insight towards metrics formulation. It should be remembered that metrics are designed according to stakeholders' objectives or goals. So having enough measures that are obtained with time and analysed or compared with other previous data can give an insight into a trend of security. For example how many intrusions are captured by the IPS/IDS at time 'x' compared to time 'y' in the previous analysis? What is the ratio of viruses prevented by anti-virus 'x' to anti-virus 'y'? Different ways of metrics derivation can be deduced from the data-set depending on the objective and purpose of a metric.

Nevertheless, metrics can be derived from the ratings aggregation results. As described in subsection 7.9, when measures are subjectively and qualitatively deduced, there is need to aggregate and average the value to get the final rate/score/value within the preset limits. The output value/score will also be used to derive new metrics from the previously obtained scores.

8
DISCUSSION

Our work has focused on what aspects are considered when measuring security. Looking at our literature review, that concentrated on industry, measurement standards and the research community, a pattern was observed on some key steps for successful security measurement. Some of these included objective setting of the measurement exercise, the threat modelling approach and the choice on whether to use a bottom-up or top-down approach.

The concept of objective setting has been discussed in the suggested measurement process of chapter 7. Common Criteria standard does suggest that good secure system engineering practice requires that the security measurement objectives are co-related to security functional requirements that were set at the development stage of the system in question. Objectives can help guide the entire measurement process, assist in data gathering and also be used in verification and validation of acquired results from the measurement. The standards, research literature and industry all alluded to these important facets of objective setting.

Threat modelling is an important aspect to consider when it comes to measuring security. Though the two are unrelated, our review has shown that to have a successful measurement programme, one needs to understand the possible threats which might lead to an attack of a given computer system. To carry out a security measurement, it is imperative to understand the possible threats that a particular system is exposed to both internally and externally and also to understand how these affect its security attributes. The interviews carried out in our review did show that most companies adopt the threat modelling concept to have a detailed understand of what aspects to measure as they seek to establish the security posture of their systems and/or environments.

A lot of the reviewed research papers also had to answer the question of whether to take the top-down or bottom-up approach when measuring security. This was also highlighted by some of the interviewees from industry. The top-down approach has the advantage of adequately mapping out the measurement plan from the set objectives. It gives a clear guideline as to what areas to concentrate on in order to have well meaning results that reflect the earlier set objective(s). However, some papers also suggested that the bottom-up approach can be used for verification and validation of the results from the measurement programme because it considers the entire scope of the system under measurement and can be streamlined to go back up to the objectives of the measurement. This notion was also strengthened by the interviewee from interview 3. After metrics have been derived, verification of metrics could be important not only to assess and verify what has been derived but also help the process of fine-tuning metrics to fit the purpose or coming up with new metrics.

Our review also shows that most of the standards used for measuring security are subjective in their approach, which introduces some level of individualism in the results reported. This might be reflected when two persons carry out measurement on the same system at different times resulting in two different sets of results. The scores/ranks are subjectively given to a particular observed factor (e.g. vulnerability, threat or breach) depending on the person carrying out the measurement. However, from our Interviews with consultancy companies, it was learned that the subjectivity is acceptable given that the person carrying out the measurement has a great understanding of security of systems and should base their subjectivity on sound security reasoning.

The security of a system or component depends on a number of different factors, thus having one solution for metrication for all possible security measurements might be difficult. Wang [23] and Voas [30] mention the multifaceted nature of security as a reason for this difficulty. A lot of attributes are involved in measuring security including the popular triad- CIA and other related dependability factors like safety, reliability, maintainability etc. The problem becomes even more complicated when more than one affected attribute can threaten the security of a single component or system and/or the occurrence of one threat can trigger more vulnerabilities. Vaos [30] suggests that if a system comprises of two components, C1 and C2, it may not always be an easy fit to have a single measure of a system due to a difference in impact on a system under a certain threat (i.e the same threat can impact the components differently).

For example, given a scale ranging from 1 - 10 with 1 representing low severity and 10 high severity, and two attributes, say availability and integrity are measured and found to be 8 and 4 respectively. Combining the two score could result into 12 which is beyond the scoring range. Taking the average results into 6 which is beyond the average value and could give a wrong impression on the overall system's security considering the scores of the individual attributes. Confusion could also arise when measures are 1 and 7 respectively. The average in this case is 4 which suggests the overall security is fair while in reality it may not be. And this goes back to the discussion of ratings aggregation of chapter 7 of this report.

In our suggested measurement process, we have proposed a way to come up with a final metric or measure that can give a more accurate picture and raise alarms on the attributes that exceed the average value of severity. This concept can help to understand the overall security posture of the entire system by also paying attention to the severity of individual components. But how do we know the overall posture of security in an organisation or system? There should be a way to quantify and combine the measures to reflect the security level of the said. More research works have not taken this into consideration and some standards observed the scenario but few efforts have been made to integrate the observation into final metrics.

9
CONCLUSION

This thesis has shown that there is still a challenge in coming up with a standard measurement/metrication model for measuring the security of computer systems and the security state of organisations. We looked at approaches adopted by research, standards and industry towards security measurement and have seen that these vary depending on the objectives and goals of the measurement.

A lot of challenges have been raised concerning the measurement of security. These include; how the objectives and goals are set, the methods followed in metric design, their implementation and reporting. This is due to different methods and approaches toward measurement and metrics formulation. There should be a way to systematise and quantify security metrics to make it easier for reporting to both technical and non technical people. Most of the standards used for measuring security are subjective in their approach, which introduces some level of individualism in the results reported.

Through this review, we found an opportunity to suggest a possible way to approach the measurement problem in a generic manner. The idea could be used to formulate and design a method that could suffice as a contribution in the search for a standard means of measuring security. The suggested measurement process could also assist the reporting process especially for executives and other stakeholders who may not understand the underlying technical details of arriving to the results of the measurement. The model achieves this by adopting the top-down approach which easily maps results to the initial objectives.

Bibliography

[1] A Complete Guide to the Common Vulnerability Scoring System Version 2.0, Peter Mell, Karen Scarfone, Sasha Romanosky, June, 2007.

[2] Radovanovic D, Sarac M, Lucic D, 2010, ‘IT audit in accordance with Cobit standard’, *MIPRO, 2010 Proceedings of the 33rd International Convention 24-28 May 2010*, IEEE, Pages 12-15.

[3] The Centre for Internet Security(1stNovember2010), "CIS Security Metrics V1.1.0" https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf.

[4] Adam R. Bryant, Captain, USAF.”Developing a Framework for evaluating organisational information assurance metrics programs“. March 2007.

[5] Payne SC. A guide to security metrics. SANS Institute Information Security Reading Room. 2006 Jun 19.

[6] Rostyslav Barabanov. “Information Security Metrics, State of the Art”. DSV Report series No. 11-007. March 2007.

[7] George K. Campbell.”Measures and Metrics in Corporate Security”. Security Executive Council Publication Series, 2011.

[8] Wayne Jansen. “Directions in Security Metrics Research”. 8IR 7564, April 2009.

[9] Joshua Franklin, Charles Wergin, Harold Booth. “CVSS Implementation Guidance”. April 2014.

[10] Dr Gary Hinson (PhD, MBA, CISSP). “A practical approach to measuring and improving information security”. In .The ISSA Journal, July 2006. http://www.noticebored.com/html/metrics.html

[11] Dr. Rabiah Ahmad, Prof. Shahrin Sahib, M.P. Azuwa.”Effective Measurement Requirements for Network Security Management”. In. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 12, No. 4, April 2014.

[12] Jennifer Bayuk and Ali Mostashari.”Measuring Systems Security”.Wiley Online Library;23 October 2012.

[13] Jonsson, Erland, and Laleh Pirzadeh. "A framework for security metrics based on operational system attributes." 2011 Third International Workshop on Security Measurements and Metrics. IEEE, 2011.

[14] Tariq, Muhammad I.”Towards Information Security Metrics Framework for Cloud Computing”.In .International Journal of Cloud Computing and Services Science,2012, vol 1,pages 209-217.

[15] Kristoffer Lundholm, Jonas Hallberg.”Design and Use of Information Security Metrics”. March 2010.

[16] Jaquith A. Security metrics. Pearson Education; 2007 Mar 26.

[17] European Union Agency for Network and Information Security.“Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report”.Feb 2011.

[18] Fylan F. Semi structured interviewing. A handbook of research methods for clinical and health psychology. 2005:65-78.

[19] Sademies, Anni. Process approach to information security metrics in Finnish industry and state institutions. Espoo: VTT Technical Research Centre of Finland, 2004. Available:http://www.sans.org/rr/papers/5/55.pdf

[20] Savola, Reijo. "A Novel Security Metrics Taxonomy for RD Organisations." ISSA. Vol. 8. 2008.

[21] Avižienis, A., Laprie, J.-C., Randell, B., and Landwehr, C.: BasicConcepts and Taxonomy of Dependable and Secure Computing. IEEE Trans. on Dependable and Secure Computing. Vol. 1, No. 1. (2004)

[22] Patriciu, Victor-Valeriu, Iustin Priescu, and Sebastian Nicolaescu. "Security metrics for enterprise information systems." Journal of Applied Quantitative Methods 1.2 (2006): 151-159.

[23] Wang, Chenxi, and William A. Wulf. "Towards a framework for security measurement." 20th National Information Systems Security Conference, Baltimore, MD. 1997.

[24] Kajava, Jorma, and Reijo Savola. "Towards better information security management by understanding security metrics and measuring processes." Proceedings of the European University Information Systems (EUNIS). 2005

[25] Savola, Reijo M., and Habtamu Abie. "On-line and off-line security measurement framework for mobile ad hoc networks." Journal of Networks 4.7 (2009): 565-579.

[26] Wang, Andy Ju An. "Information security models and metrics." Proceedings of the 43rd annual Southeast regional conference-Volume 2. ACM, 2005.

[27] Wang, Ju An, et al. "Security metrics for software systems." Proceedings of the 47th Annual Southeast Regional Conference. ACM, 2009.

[28] Sademies, Anni. Process approach to information security metrics in Finnish industry and state institutions. Espoo: VTT Technical Research Centre of Finland, 2004.

[29] Henning, R. (ed.). Workshop on Information Security Scoring and Ranking – Information System Security Attribute Quantification or Ordering (Commonly but Improperly Known as "Security Metrics), 2001, Applied Computer Security Associates

[30] J. Voas, "Why is it so Hard to Predict Software System Trustworthiness from Sofware Component Trustworthiness?," 20th IEEE Symposium on Reliable Distributed Systems, 2001, p. 179.

[31] Avižienis, A., Laprie, J.-C., Randell, B., and Landwehr, C.: BasicConcepts and Taxonomy of Dependable and Secure Computing. IEEE Trans. on Dependable and Secure Computing. Vol. 1, No. 1. (2004)

[32] Swanson, M., Bartol, N., Sabato, J., Hash, J. Graffo, L. 2003. Security Metrics Guide for Information Technology Systems. NIST.

[33] http://www.csrc.nist.gov/publications

[34] Jonsson, E. Dependability and Security Modelling and Metrics, Lecture Slides, 2015, Chalmers University of Technology, Sweden.

[35] Janusz Zalewski, Steven Drager,William McKeever and Andrew J. Kornecki,"Measuring Security: A Challenge for the Generation" Position papers of the 2014 Federated Conference on Computer Science and Information Systems pp. 131–140.DOI: 10.15439/2014F490 ACSIS, Vol. 3.

[36] Myagmar, Suvda, Adam J. Lee, and William Yurcik. "Threat modeling as a basis for security requirements." Symposium on requirements engineering for information security (SREIS). Vol. 2005.

[37] Galup, Stuart D., et al. "An overview of IT service management." Communications of the ACM 52.5 (2009): 124-127.

[38] Chew, Elizabeth, et al. "Sp 800-55 rev. 1. performance measurement guide for information security." (2008).

[39] Marianne Swanson et al., Security Metrics Guide for Information Technology Systems, NIST Special Publication 800-55, July 2003, http://cid-7086a6423672c497.skydrive.live.com/self.aspx/.Public/NIST

[40] SSE-CMM: Systems Security Engineering Capability Maturity Model, International Systems Security Engineering Association (ISSEA), referenced on July 7, 2008, http://www.sse-cmm.org/metric/metric.asp

[41] McIntyre, Annie, Blair Becker, and Ron Halbgewachs. "Security metrics for process control systems." Sandia National Laboratories, Sandia Report SAND2007-2070P (2007).

[42] Blakley, Bob. "The measure of information security is dollars.", Proceedings (online) of the First Annual Workshop on Economics and Information Security (WEIS'02), Berkeley, CA. 2002.

[43] Micrsoft threat modelling. [online], Chapter 3. https://msdn.microsoft.com/en-us/library/ff648644.aspx,

[44] Tariq,Muhammad I."Towards Information Security Metrics Framework for Cloud Computing",International Journal of Cloud Computing and Services Science,volume 1,number 4,2012,pages 209-217.

[45] Nichols Elizabeth A. and Sudbury,Andrew. "Implementing Security Metrics Initiatives",journal "EDPACS",volume 34, number 3, year 2006, pages 10-20.

[46] D. M. Nicol, W. H. Sanders, K. S. Trivedi, Model-Based Evaluation: From Dependability to Security, IEEE Trans. Dependable and Secure Computing, 1(1), 2004

[47] Trivedi, Kishor S., et al. "Dependability and security models." Design of Reliable Communication Networks, 2009. DRCN 2009. 7th International Workshop on. IEEE, 2009.

[48] Burtescu, Emil. "Reliability and Security-Convergence or Divergence." Informatica Economica 14.4 (2010): 68.

[49] Wikipedia, https://en.wikipedia.org/wiki/Splunk

[50] Herrmann, Debra S. Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI. CRC Press, 2007.

[51] Rosenblatt, Joel. "Security metrics: A solution in search of a problem." Educause Quarterly 31.3 (2008): 8-11.

[52] Alberts, Christopher, et al. "Introduction to the OCTAVE Approach." Pittsburgh, PA, Carnegie Mellon University (2003).

A

Appendix 1 - A guide to the interview questions

A GUIDE FOR THE INTERVIEW .
VERSION 1.1
16/07/2016

1.Role of the interviewee in the Company:

The idea behind this question is to try to know the right people who are involved in the process of measuring security or metrics formulation.

2. How do you measure security with consideration of some factors below?

- System modeling (a defined model as a reference to possible factors that might affect the system functionality in terms of security)
- Type of system addressed (whether its a network system, software, people or the combination)
- How do you define security (e.g minimizing risks, viruses, vulnerabilities etc) Which security aspects are covered (by considering CIA or other dependability factors)
- Measurement methodology
- Measurement scales (nominal, ratio, average, relative, absolute)
- Mathematical approach (if any)
- Type of input data (input data used to derive a metric e.g. datasets, vulnerability scan)
- Type of output metrics, e.g. quantitative or qualitative, relative or absolute, etc
- Usage of result or Application area.

The idea of asking about how the measurement process involves the mentioned and/or other parameters is to relate the parameters that other research works and standards consider with the one chosen by the organization. As it can be seen from our report, some of these parameters were the key point in paper selection. System modeling, measuring methodology, security definition, type of a system and application area of measurements or reporting are the main areas we put an efforts on.

4. Do you use metrics in measuring security?

We know measurement and metrics differ. We asked this question to know how the organization measures security. Is it for just getting a single point in view of certain factors in security or developing an analysis that will help decision making and reporting to other stakeholders within the organization. This question also opens up curiosity in asking the details on measuring process and metrication process.

5. If no, which method do you use?;

The question will help to explore more on other methods that are used to help the process of knowing the posture of security in an organization or how the organization improves efficiency and effectiveness of security procedures, processes and the like.

6. If yes, are the metrics derived by you/your company or are guided by a standard (NIST, CVSS,ISO/IEC 27001/27004):

Standards for measuring security and metrics formulation have been out for a while. They give the benchmark on how the process could be done. However, because of organization's structure differences in terms of systems, security definitions and objectives with regard to measuring security, the same methods used in one organization cannot necessarily suffice the other. So, depending on the objectives of an organization, the methods and requirement for measuring security could be customized. The question will help to know the customization done by the company or help to know how verification / validation is achieved by implementing the standards.

7. How did you arrive to those metrics? (any steps/approach and why that approach?)

This is the part of our main project, knowing different methodologies used to develop metrics or measurements.

8. How do you assess the performance or effectiveness of those metrics?:

We suggested this in the future works and as other area of interest. Verification and validation is an important process that should be thought of.

9. How do you use the metrics (organizational, operational or technical):

This helps use building the concepts on classification of metrics, reporting of metrics and knowing different stakeholders who are involved and beneficial to the process.

10. Do the metrics you are using change with the objective or system under measurement? Any criteria used to change the metrics?

The idea is to know how the company handles temporal metrics and other scenarios that may require changing the metrics previously used.

11. At the end, do you determine the posture of security of the entire system or some attributes in CIA.

Taking into consideration all the attributes and impacted attributes of security and measure the overall security of a system is still a challenge. The idea of the question is to know how the organization handles the case.