ATTACK TREE BASED INFORMATION TECHNOLOGY SECURITY METRIC INTEGRATING ENTERPRISE OBJECTIVES WITH VULNERABILITIES

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF INFORMATICS

OF

THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

BUĞRA KARABEY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

IN

THE DEPARTMENT OF INFORMATION SYSTEMS

SEPTEMBER 2011

Approval of the Graduate School of Informatics

_____

Prof.Dr. Nazife BAYKAL

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Doctor of Philosophy.

_____

Prof.Dr. Yasemin YARDIMCI

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

_____

Prof.Dr. Nazife BAYKAL

Supervisor

Examining Committee Members

Assoc.Prof.Dr.Altan Koçyiğit (METU,II)_____

Prof.Dr.Nazife Baykal (METU,II)_____

Assoc.Prof.Dr.Kemal Bıçakçı (TOBB ETU, CENG)_____

Assist.Prof.Dr.Pekin Erhan Eren (METU,II)_____

Assist.Prof.Dr.Sevgi Özkan (METU,II)_____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname: **Buğra Karabey**

Signature: **_____**

ABSTRACT

ATTACK TREE BASED INFORMATION TECHNOLOGY SECURITY METRIC INTEGRATING ENTERPRISE OBJECTIVES WITH VULNERABILITIES

Buğra Karabey

Ph.D., Department of Information Systems

Supervisor: Prof.Dr.Nazife Baykal

September 2011, 114 pages

Security is one of the key concerns in the domain of Information Technology systems. Maintaining the confidentiality, integrity and availability of such systems, mandates a rigorous prior analysis of the security risks that confront these systems. In order to analyze, mitigate and recover from these risks a metrics based

methodology is essential in prioritizing the response strategies to these risks and also this approach is required for resource allocation schedules to mitigate such risks. In addition to that the Enterprise Objectives must be focally integrated in the definition, impact calculation and prioritization stages of this analysis to come up with metrics that are useful both for the technical and managerial communities within an organization. Also this inclusion will act as a preliminary filter to overcome the real life scalability issues inherent with such threat modeling efforts. Within this study an attack tree based approach will be utilized to offer an IT Security Risk Evaluation Method and Metric called TEOREM (Tree based Enterprise Objectives Risk Evaluation Method and Metric) that integrates the Enterprise Objectives with the Information Asset vulnerability analysis within an organization. Applicability of the method has been analyzed within a real life setting and the findings are discussed as well within this study.

Keywords: Information security, risk evaluation, attack trees, enterprise objectives modeling

ÖZ

KURUMSAL HEDEFLERİ GÜVENLİK AÇIKLARI İLE BİRLEŞTİREN SALDIRI AĞAÇLARI TABANLI BİLGİ TEKNOLOJİSİ GÜVENLİK ÖLÇÜTÜ

Buğra Karabey

Doktora, Bilişim Sistemleri Bölümü

Tez Yöneticisi: Prof.Dr.Nazife Baykal

Eylül 2011, 114 sayfa

Güvenlik, Bilgi Teknolojileri (BT) sistemleri için en önemli unsurlardan biri haline gelmektedir. Bu sistemlerin ve üzerlerindeki bilginin, gizlilik, bütünlük ve de erişilebilirliğinin sağlanması, öncelikli olarak sistemlerin maruz kaldığı güvenlik risklerinin analizini gerektirmektedir. Riskleri analiz etmek, önlem almak ve gerçekleşmesi durumunda sistemleri ayağa kaldırmak için ölçüt tabanlı bir yaklaşım gerekli olmaktadır. Yine bu risklere karşı alınacak karşı koyma

stratejilerinin önceliklendirmesinde ve de bu amaç için ayrılacak kaynakların belirlenmesinde, baz alınacak bilgi güvenliği risk ölçütleri gerekli olmaktadır. İlave olarak bu ölçütlerin tanımlanmasında, etki değerlendirmesinde ve önceliklendirme esnasında Kurumsal Amaç ve Hedeflerin sürecin odağında yeralması önşart olmalıdır. Bu sayede ölçütlerin kurum içerisindeki hem teknik hem de yönetici kademelerine faydalı olacak sonuçlar üretmesi mümkün olacaktır. Aynı zamanda uygulamada bu tür tehdit modellemelerinin ortaya koyduğu ölçeklenme sorunu da kurumsal hedeflerin sürece dahil olması ve ilk aşamadan itibaren ortaya konacak çabayı önceliklendirmesi ve sınırlandırması ile çözülebilmektedir. Bu çalışma çerçevesinde Kurumsal Hedefleri ve de Bilgi Varlıklarının güvenlik riski konumunu ölçümleyen Ağaç temelli Kurumsal Hedefler ve Risk Değerleme Ölçütü adlı bir yöntem geliştirilmektedir. Yöntem, kurumsal bir ortamda kullanılmış ve sonuçları da analiz edilerek bu çalışma kapsamında paylaşılmaktadır.

Anahtar: Bilgi güvenliği, risk değerlemesi, saldırı ağaçları, kurumsal hedef modellemesi.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisor Professor Nazife Baykal, for her encouragement, support and guidance. Without her I would not even dare to set sail on this long journey.

I would also like to thank the members of my thesis committee, Assoc.Prof.Kemal Bıçakçı and Asst.Prof.Erhan Eren for their supportive feedback and creative ideas that acted as a great catalyst during my research.

I also would like to thank Sibel Gülnar and Necla Isiklar for their kindness and support.

And last but not the least, thanks to Senay and Taylan Karabey for the source code and to Doğa and Beril for lifelong inspiration.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

ALE:	Annual Loss Expectancy
ANSSR:	Analysis of Networked Systems Security
CDG:	Component Dependency Graphs
CERT:	Computer Emergency Response Team
COTS:	Commercial Off the Shelf
CVSS:	Common Vulnerability Scoring System
FISMA:	Federal Information Security Management Act
GQM:	Goal, Question, Metric
HIPAA:	Health Insurance Portability and Accountability Act
ISACA:	Information Systems Audit and Control Association
ISMLC:	Information Security Management Life Cycle
ISSEA:	International System Security Engineering Association
MORDA:	Mission Oriented Risk and Design Analysis
MTBF:	Mean Time Between Failures
NIST:	National Institute of Standards and Technology
NSA:	National Security Agency
OWA:	Order Weighted Averages
PCR:	Perceived Composite Risk

RBV:	Resource Based View
SANS:	System Admin, Audit, Network, Security
SOA:	Service Oriented Architecture
SSE-CMM:	System Security Engineering Capability Maturity Model
TEOREM:	Tree based Enterprise Objectives Risk Evaluation Method and Metric
VRIN:	Value, Rareness, Inimitability, Non-substitutability

CHAPTER 1

INTRODUCTION

Information technology systems are becoming ubiquitous in every aspect of private and public institutional work processes. So to ensure the confidentiality, integrity and availability of these systems and to protect the information residing in these systems, the discipline of IT security is gaining importance. In order to perform the duties outlined within the scope of IT security a numerical basis is essential to prioritize, judge and prepare/plan against security risks. As any other process, security cannot be managed without measurement. As the key figure in Thermodynamics, Lord Kelvin put forward;

> If you cannot measure it, you cannot improve it. In physical science the first essential step in the direction of learning any subject is to find principles of numerical reckoning and practicable methods for measuring some quality connected with it, 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 meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of Science, whatever the matter may be.

So, in order to efficiently guide and manage the IT security efforts a numerical basis is required. Also there are regulatory, financial and organizational requirements for measuring IT security performance and risk mitigation. Metrics

give institutions means to prioritize threats or vulnerabilities and the risks they present. Metrics are tools designed to facilitate decision making and improve performance and accountability and thus they must be in coherence with organizational goals and objectives. Within the National Institute of Standards and Technology, Security Metrics Guide for Information Technology Systems (NIST SP 800-55), it is stated that, by using metrics, program managers and system owners can isolate problems, justify investment decisions and focus investments to the areas where it is most needed. By using metrics to target security investments, organizations can get the best value from available resources.

Another major change in the IT world is the ever increasing interconnectivity of organizational IT resources and the pervasive exchange of information between institutions. So this multi-institutional nature of information and its exchange, presents an additional and critical level of complexity for IT security and its risk assessment. Currently the field of IT security risk metrics is at its emergence and initial growth phase, but there is a massive amount of research focused on this area due to the clear and present threats aiming the institutional IT resources in public and private sectors.

Most of the time this added complexity of multi institutional nature can be covered under the perspective of a “system of systems” and it only adds an additional layer in the abstraction process of the problem. It is evident that the metrics and especially the quantitative ones are at their infancy and of limited variety. Also the existing metrics are highly restricted to the area of technical security whereas a perspective that wholly integrates the enterprise objectives with the technical vulnerabilities is nonexistent. So we have decided to focus on the study of the development of an IT security risk evaluation method and metric that takes the Enterprise Objectives as a focal point in its build-up stages (asset selection and valuation, impact definition, vulnerability and attack scenario prioritization) and within the further calculation, execution stages of this pursuit we have decided to use the Attack Trees approach defined by Schneier (1999). Although there are

major scalability issues resultant from the application of these attack graphs and attack trees on real life information systems, we believe there will be an increase in efficiency by the usage of these enterprise objectives as a preliminary filter in identifying and prioritizing the IT assets that are the most critical ones, so that the required analysis effort can be diverted to them and even becomes limited to them. So we will be using the attack trees framework and we will also build upon this framework an analysis methodology that embeds Enterprise Objectives utilizing the Resource Based View of the corporation from the academic field of management to come up with an IT Security risk evaluation method and metric called TEOREM (Tree based Enterprise Objectives Risk Evaluation Method and Metric). As was noted by Garigue and Stefaniu (2003), security reporting remains a half science, half art skill and the challenge is to move on the fast track from art to science by selecting a security reporting framework that is aligned with business objectives.

In performing the research work that forms the basis for this thesis, we have followed a design-science approach and applied the guidelines of design-science research (Hevner, March and Ram, 2004). In line with the above outlined problem we intended to come up with a method that will resolve the issues entailed within these problem statements and will act as the "artifact" of the design-science research process. In evaluating the outcome of this process we have reverted to the "observational" (case study research) and "experimental" (controlled experiment focusing on the efficiency achieved) methods. We believe that our proposed method builds upon previous research work on the domain of information security risk assessment and also addresses the issues of managerial relevance and excessive time/effort overhead inherent within previous methods.

Our proposed method TEOREM utilizes Attack Trees within its execution however uses the Resource Based View of the company from the academic field of management, in defining the critical information assets relevant for the on-going business success of the enterprise. Essentially our design-science research process

for this information security risk assessment method is based upon kernel theories from the domains of information security and management. These are synthesized to come up with the intended qualities of efficiency/scalability and relevance.

In the chapter 2 of this thesis the literature on the research topic will be outlined. In chapter 3, the devised method will be shared that is based upon the attack tree and resource based view modelling approaches that forms the basis for the TEOREM method. In chapter 4 the research methodology and the results of the research performed will be presented and discussed. Conclusion section also entails the limitations of the study and ideas for further research on this area.

CHAPTER 2

LITERATURE REVIEW

2.1. Information security risk assessment methods and metrics

As it is impossible to eliminate all the risks, organizations may hope that perceived risk can be reduced if risk advice can be obtained through risk assessment. Therefore risk management plays a critical role in protecting an organization's information assets. Ozier's work cited in Guan, Lo, Wang and Hwang (2003) states that risk management encompasses two phases; the first phase of risk assessment, includes identification of the assets and their value, calculation of probability of each threat, evaluation of vulnerability of the assets to the threats and determine the risk level, the second phase of risk management, includes the process of assigning priority to budgeting, implementing and maintaining appropriate risk reducing measures. Roehl and Fesennmaier as cited in Guan et al. (2003) have categorized information security risk into seven items; equipment risk, financial risk, physical risk, psychological risk, satisfaction risk, social risk and time risk.

Bodeau (1992) states that the model of risk that underlies a given risk analysis methodology consists of a selected set of key concepts and associated terms, which form the vocabulary for describing risk. The most commonly used terms are system, threat, asset, vulnerability, safeguard or countermeasure, and risk; the

terms impact and outcome are also often used. Within this terminology, vulnerability is any weakness that makes an information asset susceptible to exploit by a threat, a threat is a potential cause of an unwanted impact to a system or organization and risk can be defined as the combination of the probability of an unwanted event and its consequence. So, vulnerability in itself is not enough to be considered an issue, but when this vulnerability is abused by a threat than a negative impact is generated. All in all risk management is the process of determining an acceptable level of risk, assessing the current level of risk and taking steps (mitigation) to reduce risk to the acceptable level and the maintenance of this level. A risk model not only defines terms, it also specifies which attributes of those terms are relevant and useful in assessing risk. A major modeling issue is level of detail. While too few attributes result in an oversimplified and unrepresentative model, too many details increase the cost of information gathering without corresponding benefits in greater correctness of risk analysis return (Bodeau, 1992). As was stated in Bennett and Kailay (1992) a variety of risk analysis methods have been developed and usually conform to the following steps, which form a framework for risk analysis:

- Identification of the components that make up the system as a whole (hardware, software, information),
- Identification of risks to which an organization might be exposed,
- Identification of weaknesses or vulnerabilities that exist within the system that could allow the realization of any or all of the identified threats,
- Identification of existing security controls, both technical and managerial, and their degree of enforcement,
- Assessment of the effects or impacts of those risks, which have been identified on the organization so that the value of avoidance or reduction can be assessed.

Guan et al. (2003) define these steps as;

- System characterization,
- Threat identification,
- Vulnerability identification,
- Control analysis,
- Likelihood determination,
- Impact analysis,
- Risk determination,
- Control recommendations,
- Results documentation.

These are also summarized as perimeter definition, asset identification and characterization, threat identification, risk evaluation, countermeasure definition and application and residual risk evaluation (Aime, Atzeni and Pomi, 2008).

Also as was stated in Patriciu, Priescu and Nicolaescu (2006), historical data can act as a metric. These metrics include the numbers of vulnerabilities found in network scans, known incidents reported, estimated losses from security events, security bug discovery rate in a new software application, intrusion detection system alerts, number of virus infected e-mails intercepted and others.

Bodeau, (1992) defines threat scenario analysis as an alternative. In this analysis scenarios are considered in which an individual interacting with a given system exploits a connection to cause events to occur on a second system. A threat scenario has two associated measures; likelihood of initiation and likelihood of impact. Likelihood of initiation depends on the attacker's expectations, while likelihood of impact depends on the attacker's capabilities and on the system safeguards.

At a more simplistic and practice oriented manner McCumber (2004) comes up with the depiction of an information security cube depicted in Figure 1 that helps the upper management visualize risk assessments for information systems.

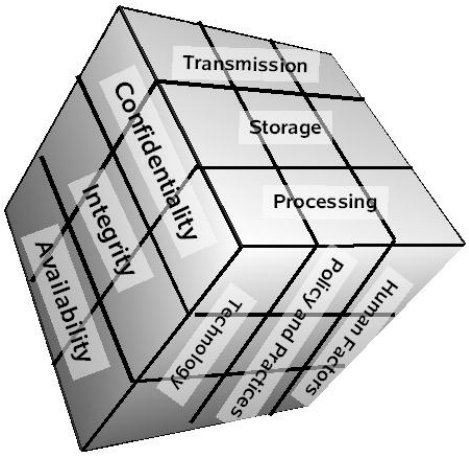


Figure 1 McCumber's cube for risk assessment (2004)

Basically there are two approaches to security metrics; qualitative and quantitative methods. Bennett and Kailay (1992) define the quantitative approach as the methods that assume it is possible to associate a level of risk with each hazard identified and attempt to calculate the value of the likely damage should risk become reality. Focus is the production of an Annual Loss Expectancy (ALE) figure, which is calculated for each threat by establishing two factors:

- Its probability of occurrence over a specified time period,
- Amount of loss that would be incurred.

These quantities are multiplied to obtain the estimated ALE, which is compared with the cost of suitable countermeasures. The philosophy here is that if the cost of a countermeasure is less that the calculated ALE then implementing the countermeasure would be a cost effective solution, otherwise alternative solutions should be considered.

However some studies criticize the ALE approach as being one dimensional and try to enhance it through various means. The approach of using the expected loss due to a breach as the ranking criterion gives the analyzer a narrow analysis of the alternatives and may lead to misleading results. PCR (perceived composite risk) is one of these alternative approaches and for a given set of information security activities PCR proposes a linear combination of the expected loss, the expected severe loss and the standard deviation of loss that can be attributable to this breach. (Bodin, Gordon and Loeb, 2008).

Bennett and Kailay (1992) also define qualitative methods as the approaches that assess risks on the basis of the capability to identify threats and vulnerabilities correctly. Unlike the quantitative approach, precise values are not sought and risks are expressed in terms of descriptive variables such as “high”, “medium”, “strong”, “weak” etc. the rationale being that the consequences of some types of loss, corruption or modification of data cannot be expressed in terms of monetary value or discrete events.

These basic approaches have been expanded by other researchers. As an example the qualitative approach has been further developed by Guan et al (2003) utilizing the Fuzzy Theory to further improve the adequacy and precision of linguistic variables. A triangular fuzzy number scheme has been employed for the linguistic variables. Since the cognition and stance of each evaluator varies, and the definition of the linguistic variables differs as well, this study has employed the notion of average value so as to integrate the fuzzy judgment value of the evaluators.

Savola (2007) further details the taxonomy for metrics;

- Quantitative vs qualitative metrics, as was discussed above,
- Objectivity vs subjectivity of metrics. The goal of security metrics development is to find metrics that are as objective as possible. As security

contains a lot of human behavioral aspects many metrics tend to be highly subjective,

- Direct vs indirect metrics. A direct measure is a measurement of an attribute that does not depend upon a measure of any other attribute. On the other hand, an indirect measure is derived from measures of one or more other attributes,
- Static vs dynamic metrics. Dynamic metrics involve time and static ones do not. Time perspective is important in security metrics as the information security threat perspective is constantly changing,
- Absolute vs relative metrics. Absolute metrics do not depend on other metrics, whereas the relative ones do.

Another approach is the quantitative ANSSR (Analysis of Networked Systems Security Risks) methodology developed by Mitre Corporation (Bodeau 1992). In ANSSR, risk is expressed quantitatively and a fairly simple summary algorithm has been utilized. However this algorithm was based upon more complex algorithms for specific events in threat scenarios. ANSSR only focuses on disclosure risk (so the confidentiality part of the confidentiality, integrity, availability trio). A high level model depicted in Figure 2 below outlines the components of risk.

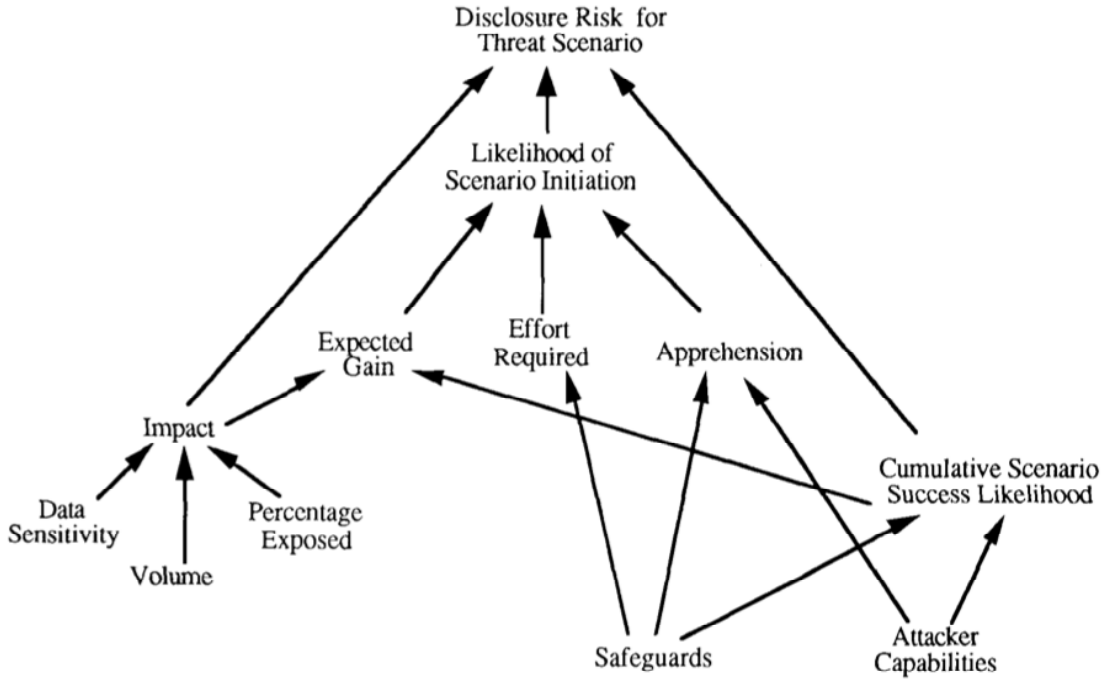


Figure 2 Components of risk (ANSSR Model) by MITRE corporation (1992)

In ANSSR model the disclosure risk is associated with an individual threat scenario. The risk associated with a threat scenario is a combination of three components:

- Likelihood that an attack exploiting that scenario will occur,
- Likelihood that the attack (represented by the threat scenario) will result in an adverse impact,
- Severity of that impact.

Impact severity depends on the assets involved. Impact associated with the disclosure of a data set depends on;

- Sensitivity of the data in that data asset,
- Total amount of data in the data asset,
- Percentage of data in the data asset that is disclosed due to the attack.

ANSSR adds to that factors such as likelihood of scenario initiation that is contingent upon relative expected gain factor, work factor, apprehension factor etc. then uses Expected Loss with Replacement formulation to come up with a result. However the shortcomings of this model are its focus on disclosure (only) and its avoidance of human errors (focusing only on deliberate attacks).

Bennett and Kailay (1992) compare the quantitative and qualitative methods and propose the advantages of quantitative methods in the ability to relate expenditure to threat value in percentage terms and to direct resources proportionally. However even though a single figure such as an Annual Loss Expectancy is an easily perceived summary of the cost of threats, it must be recognized that it is derived from data and probabilities which frequently do not have a strong empirical basis. As IT security threats are relatively recent and are constantly evolving, usage of such figures by their face values only, may present faulty conclusions.

A major advantage of the qualitative approach according to Bennett and Kailay (1992) is that the time and expense required to make the assessment is optimal. Quantitative approach usually requires an in depth and extensive study of the system/organization in order to establish threats and vulnerabilities, to determine probabilities and obtain cost figures. On the other hand, qualitative methods can usually be completed in less time with a smaller number of staff as they do not require the same type of precise data collection and mathematical calculations. However the usage of linguistic variables (that are usually subjective by nature) is a hindrance for qualitative approaches and must be further refined as was mentioned before in the case of Guan et al.'s (2003) usage of Fuzzy theory for refinement.

Yang, Boehm and Wu (2006) are also from the proponents of qualitative metrics and they devise a methodology in which a Delphi method based platform is utilized. In this method the expert opinions are compiled and reassessed in iterative ways using the Delphi method.

Another much referenced vulnerability metric is the Common Vulnerability Scoring System (CVSS) by National Institute of Standards and Technology (NIST) and Carnegie Mellon University (Mell, Scarfone and Romanosky, 2007). It is an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of three groups; Base, Temporal and Environmental. Each group produces a numeric score ranging from 0 to 10 and a Vector, a compressed textual representation that reflects the values used to derive the score. Base group represents the intrinsic qualities of vulnerability. Temporal group reflects the characteristics of vulnerability that change over time and the environmental group represents the characteristics of vulnerability that are unique to any user's environment. So CVSS is a quantitative measure to address and specify various system vulnerabilities and it also takes the dimension of time and specific context of a user organization into account. As itself it is not a risk security metric but CVSS can be utilized within the framework of a security risk methodology as a tool to quantify various vulnerabilities. Below in Figure 3 is a schematic outlining the metric groups in CVSS;

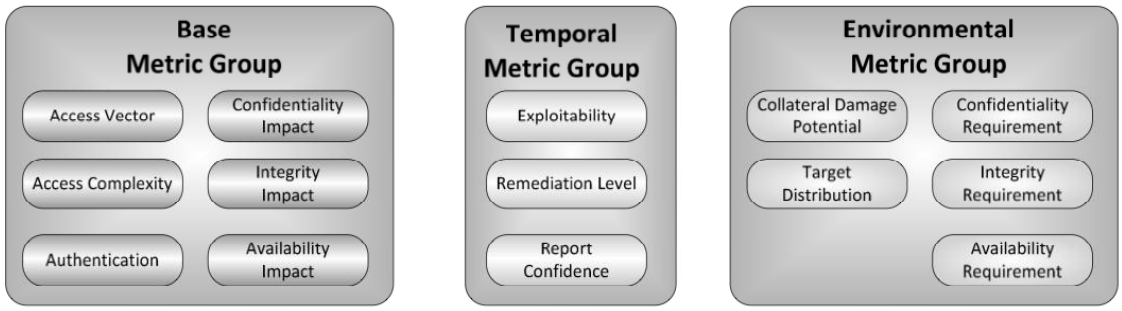


Figure 3 CVSS Metric Groups by NIST and Carnegie Mellon University (2007)

Another NIST led effort is the National Vulnerability Database which acts as a knowledge repository for many measurement and metric activities (Ahmed, Shaer and Khan, 2008). A similar reference list is the famous "bugtraq" that acts as a

reference point for security professionals. In order to probe the vulnerability status of any component automated tools like Satan or Nessus are utilized.

Current approaches to the information security risk metrics recommend and employ estimates for such critical factors as attack frequency and countermeasure effectiveness as no clear and accepted framework exists for the real world measurements of these parameters (Baker, Rees and Tippett, 2007). Also these measures tend to be geared toward the security professionals and most of the times are not suitable for managerial decision making. The security measures involved are more commonly driven by compliance mandates rather than by the principles of risk management. However the ability to calculate risk through real world metrics has far reaching implications for managerial decision making as an extension of it is in evaluating the potential return on investment of proposed security initiatives (Baker, Rees and Tippett, 2007).

US National Security Agency (NSA) developed a tool called Mission Oriented Risk and Design Analysis (Morda) and this provides a framework for analyzing complex IS risk postures. Morda combines threat, attack and mission impact concepts to derive an unbiased risk metric. Methodology outlined in Figure 4 also helps systems security engineers discover system deficiencies and develop reasonable design strategies to build stronger systems (Saydjari, 2004).

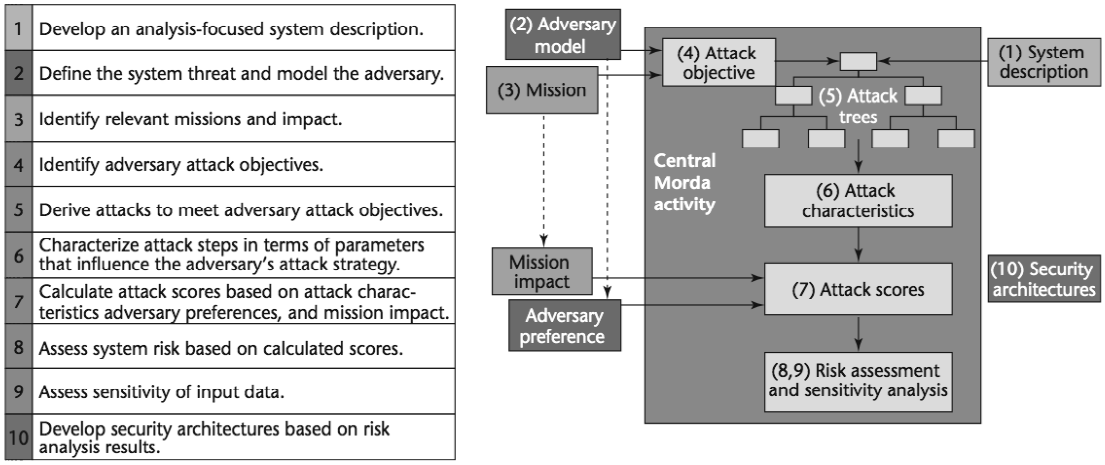


Figure 4 Morda Assesment Process Steps (includes Attack Trees approach) by NSA

MORDA has further been refined by the works of Evans and Wallner (2005). Their work is based upon the modification of the security subset of the overall MORDA process.

There are a number of other vulnerability scoring systems managed by both commercial and non-commercial organizations. For example CERT/CC produces a numeric score ranging from 0 to 180, SANS vulnerability analysis scale and Microsoft's Relative Attack Surface Quotient are some other examples. While useful these scoring systems provide a one size fits all approach by assuming that the impact for vulnerability is constant for every individual and organization (Mell, Scarfone and Romanosky, 2007).

Most information systems are of a distributed nature that spans geographies or organizational boundaries. In the works by Wood, King and Kennon (2003), Hallberg, Hunstad and Peterson (2005), Bagheri and Gorbani (2007) this multi institutional perspective is covered by a "system of systems" paradigm and by the addition of one more layer during the abstraction and boundary definition process.

Risk analysis is also proliferating in the software industry as is outlined by Verdon and McGraw (2004). Investigating these methodologies may also be beneficial for our pursuit on the IT system security risk metrics. Risk analysis methodologies for software fall into two basic categories; commercial and standards based. These basic methodologies view risk from different perspectives, such as;

- Financial loss methodologies that seek to provide a loss figure to balance against the cost of implementing various controls,
- Mathematically derived "risk ratings" that equate risk with arbitrary ratings for threat, probability and impact,
- Qualitative assessment techniques that base risk assessment on anecdotal or knowledge driven factors.

So it seems that risk analysis in the software domain is taking parallel steps to the developments in the IT Security Risk Metrics community. Also the prototypical analysis for software security risks as per Verdon and McGraw (2004) mimics their counterpart in the IT Systems security domain that we have shared above;

- Learn as much as possible about the analysis target,
- Discuss security issues surrounding the software,
- Determine the probability of compromise (mapping out attack scenarios for vulnerability exploitation and balancing controls against threat capacity),
- Perform impact analysis,
- Rank risks,
- Develop a mitigation strategy,
- Report findings.

There are even suggestions to devise security patterns embedding security metrics to be utilized during the software development lifecycle by the developer community (Heyman, Scandariato, Huygens and Joosen, 2008). Similar work exists by Nyanchama (2005) in which the enterprise vulnerability management utilizing metrics is integral in the Information Security Management Life Cycle (ISMLC) process.

Although standardized security metrics are gaining increasing popularity as was stated by Patriciu, Priescu and Nicolaescu (2006), within the context of industry standards such as BS7799, ISO17799, NIST SP800-33 and the ISO 27000 family, standardized "risk metrics" are still non-existent. Within the ISO27000 family of standards the ISO27004 will be focused on security metrics and will be integrated with the ISO27001 security management standard. Although it is envisioned that in its final version ISO27004 will define a series of core metrics, there will also be guidance to devise additional customized metrics that will be required by the tailored needs of organizations.

Mention of metrics can also be found within the compliance frameworks in financial sector, healthcare, personal privacy and homeland security. Herrmann (2003) outline the current security and privacy regulations that are widely used as;

- Financial: Gramm-Leach-Bliley Act, Title V,
- Financial: Sarbanes-Oxley Act,
- Healthcare: Health Insurance Portability and Accountability Act (HIPAA),
- Healthcare: Personal Health Information Act,
- Personal Privacy: Data Protection Directive –EU,
- Personal Privacy: Data Protection Act –UK,
- Personal Privacy: Privacy Act –US,

- Homeland Security: Federal Information Security Management Act (FISMA),
- Homeland Security: Patriot Act.

Similar harmonization efforts are for a long time under discussion also in the European Union (Wood, 1990). They also focus mainly on providing sets of controls, but the measurement of the quality and applicability of these controls are not handled in detail. In other words they focus on the "policy" aspects of security. In the same study Security Metrics Consortium (SecMet) was referenced, however this industry/vendor driven consortium could not come up with conclusive results since its inception in 2004. Also a Common Criteria based measurement schedule has been proposed by Hunstad, Hallberg and Andersson (2004).

Another standardization effort is led by the Metrics Work Group of International System Security Engineering Association (ISSEA). This group is tasked to develop metrics for Systems Security Engineering – Capability Maturity Model (SSE-CMM). SSECMM has adopted the NIST 800-55 methodology of developing security and process metrics.

Another perspective at looking at risk is in order to identify "risk based benefits" as was put forward by Arora, Hall, Pinto, Ramsey and Telang (2004). They define risk based benefit as the reduction in expected loss from security failure incidents which does not necessarily translate into additional resources which companies would typically use for other productive endeavors.

As a final resort we have investigated the IT security risk metric approaches in the insurance community. Magnusson and Yngstrom (2004) have investigated the methodology behind the insurance database Estimated Maximum information technology Loss (EMitL) that is widely used around the world by the insurance companies. Insurance policies cover different types of risk; business interruption, fraud and embezzlement, robbery and theft, defamation, infringement of privacy,

infringement of trademark. EMitL is based upon a qualitative assessment of the IT security awareness and maturity of the organization at hand.

When we investigate the required qualities of a metrics system we may refer to Brotby (2009) who outlines the positive attributes of metrics as;

- Manageable,
- Meaningful,
- Actionable,
- Unambigous,
- Reliable,
- Accurate,
- Timely,
- Predictive.

So we will be trying to come up with the above listed qualifications within our proposed metric.

A potential reason underlying the fact that limited information is available in developing these methods or of improving existing ones as was stated by Papadaki and Polemi (2007) may be the organizations' preference to keep this information confidential. Also the development of these methods is rather an ad hoc than a systematic process in most cases. Papadaki and Polemi (2007) propose that whichever the reason might be, it is evident that there are not sufficient research efforts regarding the systematic development of information security risk management methods, unlike other fields.

However the proper definition in line with the Enterprise Policies and Objectives of this risk and also its right quantification is essential for business success. As was quoted by Rowley (1989) as the notion of "Right Risk";

> The whole of business is about taking an acceptable risk. Companies that take no risk disappear. Companies that take unacceptable risk plainly also disappear. The problem is therefore invariably to minimize the risk that can be minimized, while taking quite high levels of risk in areas which cannot.

As was quoted by Breu, Oberperfler and Yautsiukhin (2008) the increasing dependency of core business processes on IT is transforming the IT Security Management to the "Board Rooms" of enterprises. So it is evident that a proper security metric must also embed within itself the perspective of enterprise level goals and objectives.

2.2. Main objectives of the devised method

During the literature survey for the IT Security Metrics we have usually come up with metrics that quantify the risk by taking into account the probability of occurrence and the impact, both components of this calculation have shortcomings;

- Due to the limited availability of statistics on the area of IT security, probabilistic calculations that are built upon historical data may not be reliable,
- Due to the evolving nature of IT security threats and vulnerabilities, there may be asymmetric or non-linear leaps in the threat domain, compared to the traditional defense systems, so the threats were dynamic in nature.
- When we take the impact into account, there are lots of "intangible" components of the assets that are at stake. So taking into account the technical level or pure monetary losses (only) will not cover all bases. Also the business goals and priorities must be included in the model.

- Most of the time the end result of IT security assessments address the technical community, whereas the management community are also in a position to digest these results and utilize them within their decision making processes on risk mitigation and investment decisions.
- Due to the cascaded and/or parallelized nature of IT components and networks (especially in multi-institutional systems) a "systems approach" must be embedded in the analysis. As was stated by Yngstrm (2003) a systems-holistic approach is required to analyze the risks involved in such interconnected, and frequent data sharing domains like multi-institutional environments.

Upon additional literature research it was concluded that the first two issues above can be addressed by a technique called Attack Trees which will further be detailed below. As was stated by Bennett and Kailay (1992) unlike the risks which focus on losses arising from financial claims, system security risks are of a more involved nature which can only be evaluated by considering a complex combination of possible consequences and attack trees are well suited for this endeavor. Moreover, system security risks are not readily specified in pure monetary terms as was outlined in the third issue above. Potential losses are often related to factors such as corporate goodwill or other non-monetary assets and for example the extent of loss in customer confidence following a security breach is extremely difficult to quantify before the event. Not only is it difficult to put a precise financial value to a wide range of threats but it is common for people to be unwilling to assign a monetary measure at all in situations where threats have a social impact, for example in the disclosure of confidential medical records. High risk organizations may even adopt a "security at any price" policy.

Requirement for the end results of such assessments to be useful and to be utilized by the management community necessitates the analysis process to be in line and in synchronization with enterprise goals and objectives.

As a result we have decided to come up with a methodology which utilizes past and current management research on Resource Based View (RBV) for organizations to identify the resources essential for a firm's success in line with its Enterprise Objectives and this methodology further maps these resources and thus the Enterprise Objectives with the Information Assets domain. We will focus in detail on this in the upcoming sections.

Also regarding the fifth issue above, we have come to the conclusion that the interlinked, connected in parallel, multi institutional domains can be considered as a "system of systems" and this will only add an additional layer to the abstraction process. So we have focused our research on the pursuit of devising an IT security risk evaluation method and metric that integrates the Enterprise Objectives (and their relevant resources) into the process and utilizes the Attack Tree methodology as the basic mechanism. So in the end the multi institutional perspective will be served by an "attack forest" that integrates individual attack trees.

An interesting research is implemented by Clark, Dawkins and Hale (2005) that tries to address the challenge of "fusing the enterprise objectives and vulnerabilities". Within their research they have blended the pure technical vulnerability scanning with a mapping that puts the enterprise objectives into context with these vulnerabilities. They state that, although it is essential to risk management, little agreement exists concerning the generation and usefulness of security metrics. Conventionally some risk assessment techniques engage policy based metrics (such as the maturity based approaches), but by only evaluating high level policies and procedures these methods do not assess technical flaws in security. On the other hand the technology focused evaluation methods cannot understand the business impact with respect to an organization of a vulnerability being exploited. So Clark, Dawkins and Hale (2005) propose a fusion approach utilizing a mission tree to identify mission valuation and match these objectives with vulnerabilities to come up with a metric figure. In their model they suggest that through interviewing management and the review of mission statements the

customer needs will be identified and further these goals will act as the focal point of a risk assessment that will utilize mission trees.

In the mission modeling phase of their approach they depend on in depth discussions and interviews with the management team of the organization. After this step the entities on the mission tree and the related weights are defined. Afterwards, a professional vulnerability scanning tool scans the system and threats to the objectives (and to the assets that form a basis for these objectives) in the mission tree are identified. So summing up the scores for these vulnerabilities a final score is achieved. However their approach only takes into account one aspect of the organizational risk (vulnerability measured by off-the-shelf scanners) however there are numerous other criteria that can be embedded in a proper metric such as attack costs, adversary resources, adversary's perceived benefits, attack scenario's relative probability, victim's per incident loss, victim's perceived impact etc. Also in their methodology the upper most goals are assumed as given, however this phase may also be included in the methodology as this is the most critical and focal aspect of this approach that blends, fuses, integrates the enterprise mission, business goals and objectives with the information assets under potential attack. Further to this study Clark, Singleton, Tyree and Hale (2008) put forward a model called Stratagem that attempts to put mission modeling within the focus of risk assessment as well.

Breu, Oberperfler and Yautsiukhin (2008) also underline the importance of fusing the business level objectives with the technical level IT security issues. Below in Figure 5 and Figure 6 is a depiction of their enterprise level modeling and further its process level breakdown to be utilized as a basis for risk analysis.

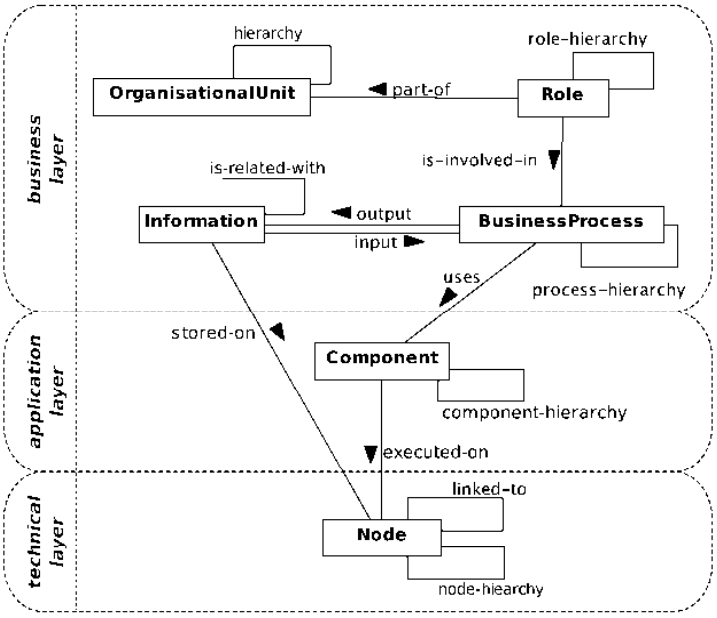


Figure 5 Enterprise meta model by Breu et al. (2008)

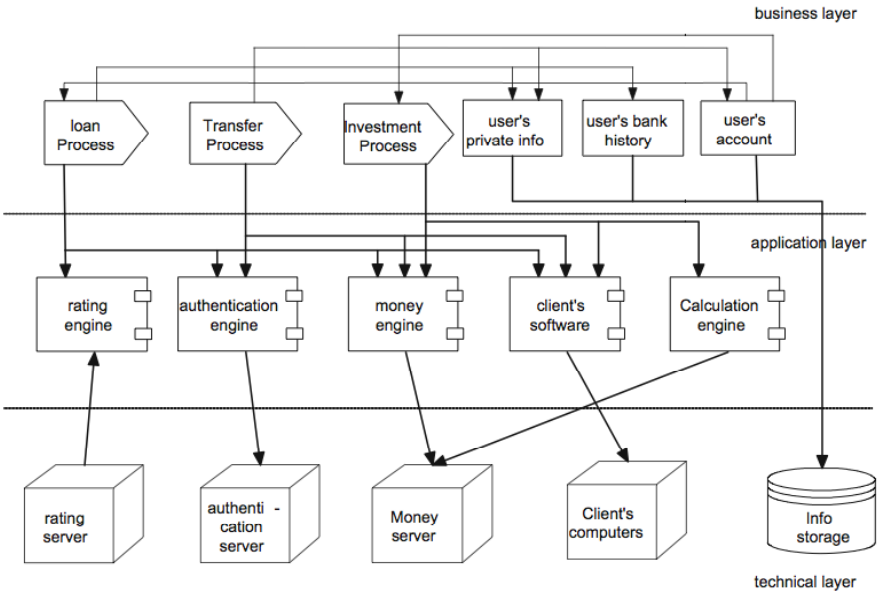


Figure 6 Enterprise model of a bank's IT architecture by Breu et al (2008)

Breu, Oberperfler and Yautsiukhin (2008) use this breakdown to define the linkages between the business layer and technical layer. Although they utilize

dependency graphs in their risk analysis they further limit the graph structure to avoid cycles both in business level and technical level so their approach closely approaches a tree structure in the end.

ISACA (Information Systems Audit and Control Association) is a professional organization focusing on the area of information audit and control. Recently they came up with a framework called RiskIT that entails all the aspects of information security risk assessment and governance. Also in their Risk IT framework depicted in Figure 7 they have envisioned the business objectives at the center of the process although the inner workings are not explicitly defined and left for the user of the framework to define and utilize.

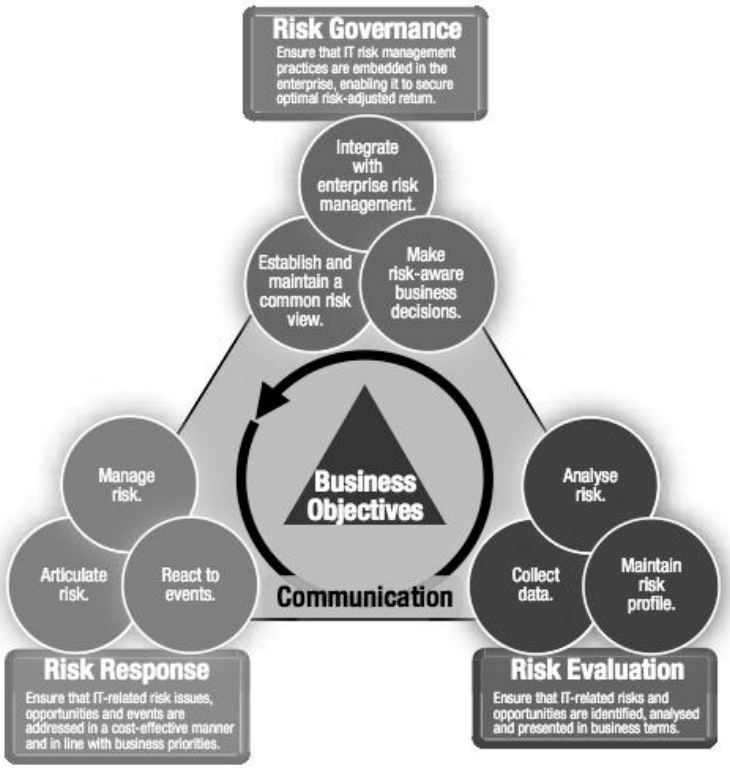


Figure 7 Risk IT Framework by ISACA (2009)

So our challenge will be to come up with this methodology that calculates a risk metric taking into account a multi-faceted parameter space and keeping at its focus

the enterprise objectives as the ultimate serving point for the information assets under the threat. In doing so we will utilize the attack tree modeling methodology together with the resource based view modeling approach from the management domain.

2.3. Attack Trees

IT Security Risk analysis is not the first risk discipline to use tree structures. Fault or failure trees have long been used to understand how component failures do affect the overall systems functioning. In the discipline of fault tree analysis failures stemming from the system itself due to reliability issues (MTBF) and also the environmental effects are at the center stage.

In the attack tree analysis the attack trees are built from the perspective of the attacker instead of the defender (Amenaza Technologies Ltd., 2008). Attack tree models are very well suited at estimating the risk for situations where such occurrences of multi-step and pre-planned malicious activities take place.

Purpose of an attack tree is to define and analyze possible attacks on a system in a structured manner; structure is expressed in a node hierarchy, allowing the decomposition of an abstract attack into a number of more concrete attack steps (Mauw and Oostdijk, 2005).

Attacks are usually modeled through the use of a graphical, mathematical, decision tree structure called an attack tree. Initial reference to a similar structure was by Weiss (1991) in a paper describing “threat logic trees”. Amoroso (1994) further detailed a modeling concept called threat trees and most recently Schneier (1999) put forward the idea of utilizing an attack tree for this purpose and further elaborated it in his book (Schneier, 2000). In his initial work on the subject Schneier (1999) defined a tree as a formal, methodical way of describing the security of systems, based on varying attacks. Goals are noted as the root nodes and different steps to achieve this goal are denoted as leafs. In his work also values

have been assigned to the steps as I (Impossible) or P (Possible) and nodes are defined as either AND notes or OR nodes. As was pointed out by Moore, Ellison and Linger (2001) most of the time attack trees take the form of an attack forest for enterprise wide threat analysis.

Attack trees were further enhanced by some studies like Yager (2005). In this study Yager proposes the usage of Order Weighted Averages (OWA) as an extension to the AND/OR nodes of attack trees. Thus a probabilistic uncertainty can be added within the tree model.

Concept of attack trees were further developed by other researchers. Mauw and Oostdijk (2005) criticized the current state of attack trees by lacking the required formalism and tried to put together an approach that defines the rigorous formalism for the attack trees, involving mechanism for reduction and normalization of the trees.

Gan, Jiufei and Wu (2007) came up with an extended attack tree in which they have defined an additional node type as the conditional and, in addition to that utilized “utility curves” from the multi attribute theory to convert the parametric scores for the attackers value based utility behavior, technical ability function as can be seen in Figure 8, Figure 9 and Figure 10. Extended attack trees and the utility curves are embedded in commercial attack tree tools immediately (Amenaza Technologies Ltd., 2008).

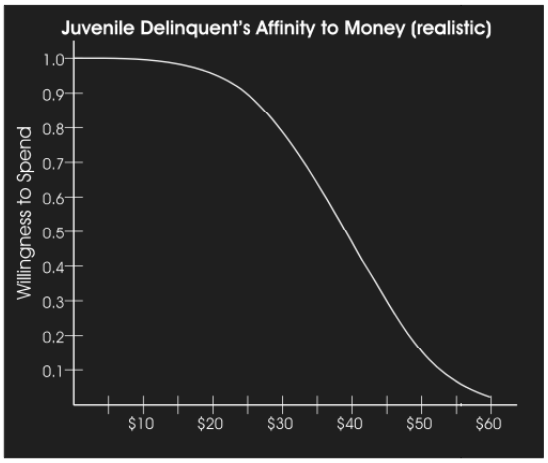


Figure 8 Value based agent profile by Amenaza Technologies (2008)

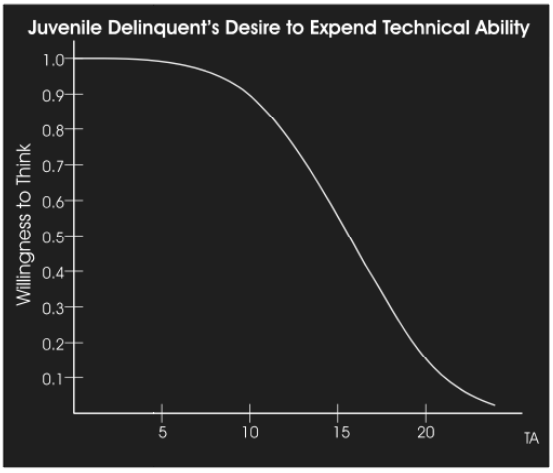


Figure 9 Juvenile attackers technical ability utility function by Amenaza Technologies (2008)

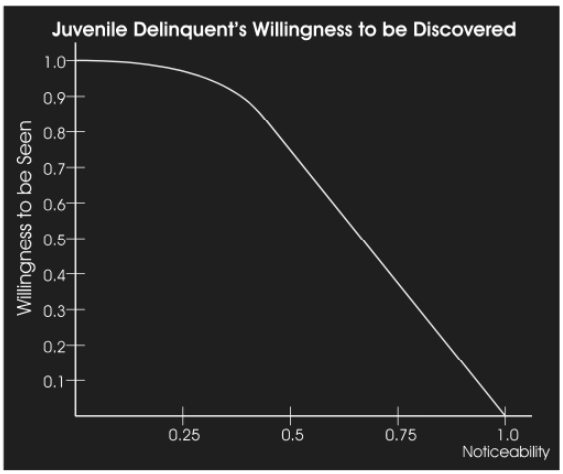


Figure 10 Juvenile attackers noticeability utility function by Amenaza Technologies (2008)

When such additional perspectives and utility functions are added to the Schneier's basic attack trees we come up with a more holistic attack tree attribute flowchart as can be seen below in Figure 11 (Ameneza Technologies Ltd., 2008).

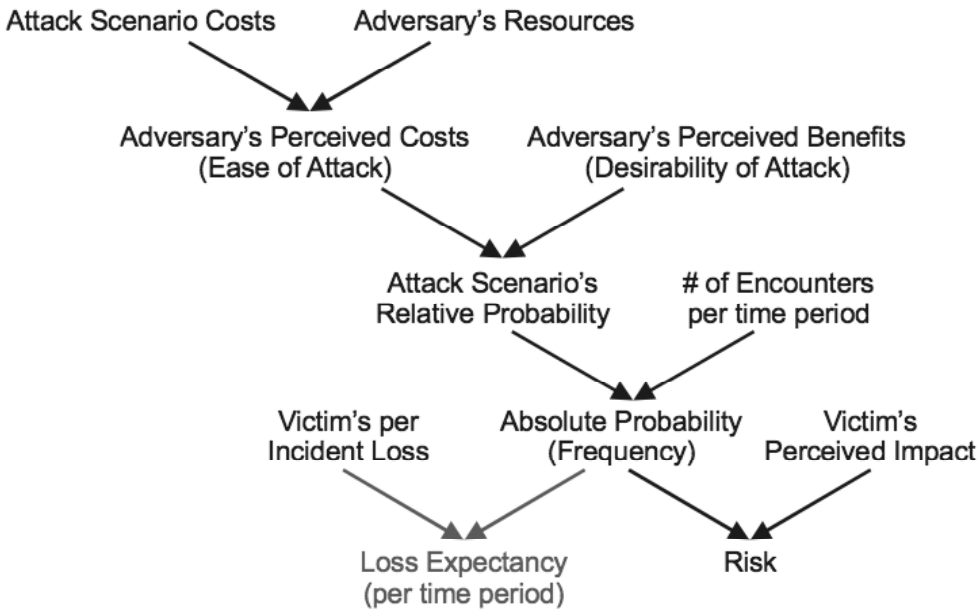


Figure 11 Hostile Attack Risk Analysis Flowchart by Amenaza Technologies (2008)

SecurITree tool by Ameneza Technologies can help one to draw very complex conclusions using capability based modeling. It allows an analyst to describe possible attacks against a system in the form of graphical, mathematical model as an Attack Tree. The capabilities of motivated attackers are compared with the resources required to perform specific attacks in the model through pruning and the attacks that are beyond the capabilities of the attacker are removed from the model (Duan, Saini and Paruchuri, 2008).

Different attacker profiles and the inclusion of this criterion to the analysis is another research topic that has been investigated by Grunske and Joyce (2007). Their work takes into account the attacker heterogeneity when performing security evaluations using attack profiles.

Additional work on the area of attack trees has been performed by Sahinoglu (2005). In his work he uses the basic notion of attack trees but focuses on the concept of the lack of a countermeasure for quantifying the analysis and uses a probabilistic model and comes up with a metric called Security Meter. In his work a Monte Carlo analysis has been performed to check the viability of this model.

Within some other related work the term attack graphs have been utilized (Phillips and Swiller, 1998) in which the event sequences are the focal point rather than the event abstractions and other tools like reachability analysis take the center stage. Also it is worth mentioning that provided that we permit the sharing of the nodes as a means to express a sub-attack's occurrence more than once and we do not allow construction of cycles, our trees become essentially rooted directed acyclic graphs (Mauw and Oostdijk, 2005).

In their work, Phillips and Swiler (1998) criticize fault trees as not modeling cycles such as an attacker starting at one machine, hopping to two others, returning to the original host, and starting in another direction at a higher privilege level. Ammann, Wijesekera and Kaushik (2002) suggest thinking the attack tree as a structure in

which each possible exploit chain ends in a leaf state that satisfies the attacker's goal and an attack graph as a consolidation of the attack tree in which some or all common states are merged. They also state that with attack graphs the analysis pursuit most of the time becomes too large to be practical whereas with attack trees the same goal can be achieved with only the cost of monotonicity. Monotonicity means that no action an attacker takes interferes with the attacker's ability to take any other action which is a reasonable modeling assumption in most network analysis cases.

Similar work has been performed utilizing component dependency graphs (CDG) that were developed earlier for reliability analysis (Yacoub, Ammar and Robinson, 2000). Component Dependency Graphs are used as probabilistic models in reliability analysis at the architecture level to analyze the reliability of distributed component based systems. CDG's are directed graphs that represent components, component reliabilities, link and interface reliabilities, transitions and transition probabilities. They are derived from scenarios.

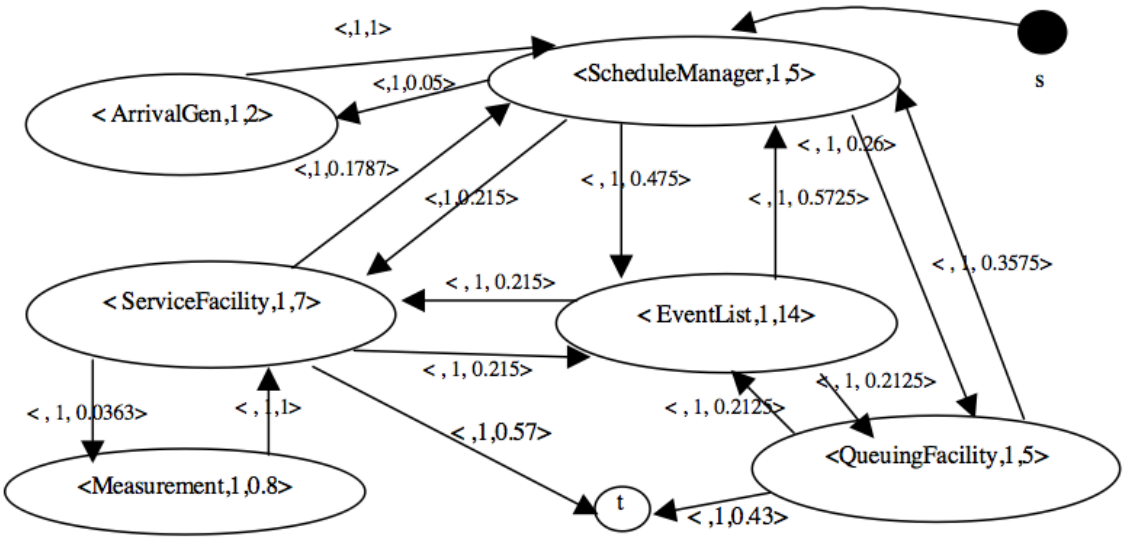


Figure 12 CDG of a Pacemaker by Yacoub et al (2000)

Same methodology outlined in Figure 12 is utilized for reliability analysis in Component Based Software applications (Yacoub, Cukic and Ammar, 2004), however its usage in attack analysis is limited due to its scalability issues and the flexibility provided by the multi attributed nature of extended attack trees.

Khand (2009) offered the usage of different types of nodes within the attack tree to widen the usage of them and to address the issues related with the redundancy mechanisms, fault and error recovery mechanisms that necessitate a state based nature such as PAND node, k/n node, SEQ node and CSUB node. However we believe such approaches may further complicate the process and add up to the scalability issues with the attack trees.

A similar extension to the usage of attack trees has been done by Dewri et al (2007), within which they have approached the problem of optimal security hardening of a system as a multi-objective optimization problem on an attack tree model of the system and used evolutionary algorithms to solve it.

Also an interesting usage of attack trees is on the field of privacy. Reddy, Venter, Olivier and Currie (2008) utilize the attack trees in the analysis of privacy problems. Their method called privacy taxonomy based attack tree analysis involves the combination of privacy violation taxonomies and attack trees. It assists organizations in protecting information privacy by providing a means to analyze weaknesses in their protective measures from the perspective of privacy rather than security.

As was mentioned before Attack Trees are a good fit for analyzing distributed systems in which the information technology resources are spread either geographically, physically or between different organizations. Fung et al (2005) discuss the survivability analysis of distributed systems using attack tree methodology in their study. They also note that especially within domains in which

SOA (Service Oriented Architecture) is utilized, the attack tree methodology offers valuable insights.

Practical usage of Attack Trees has been investigated by Edge, Raines, Grimaila, Baldwin, Bennington and Reuter (2007). Within their study the use of attack and protection trees to analyze security for an online banking system has been performed and the results are discussed. In the Figures 13 and 14 below the resultant online banking attack and protection trees are depicted.

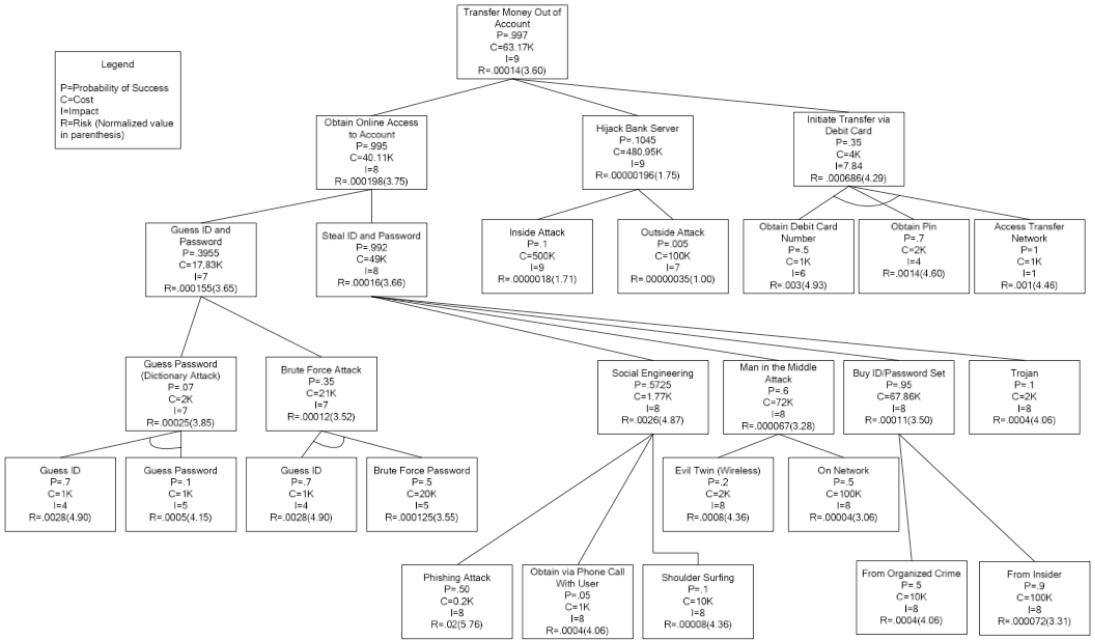


Figure 13 Online banking attack tree by Edge et al (2007)

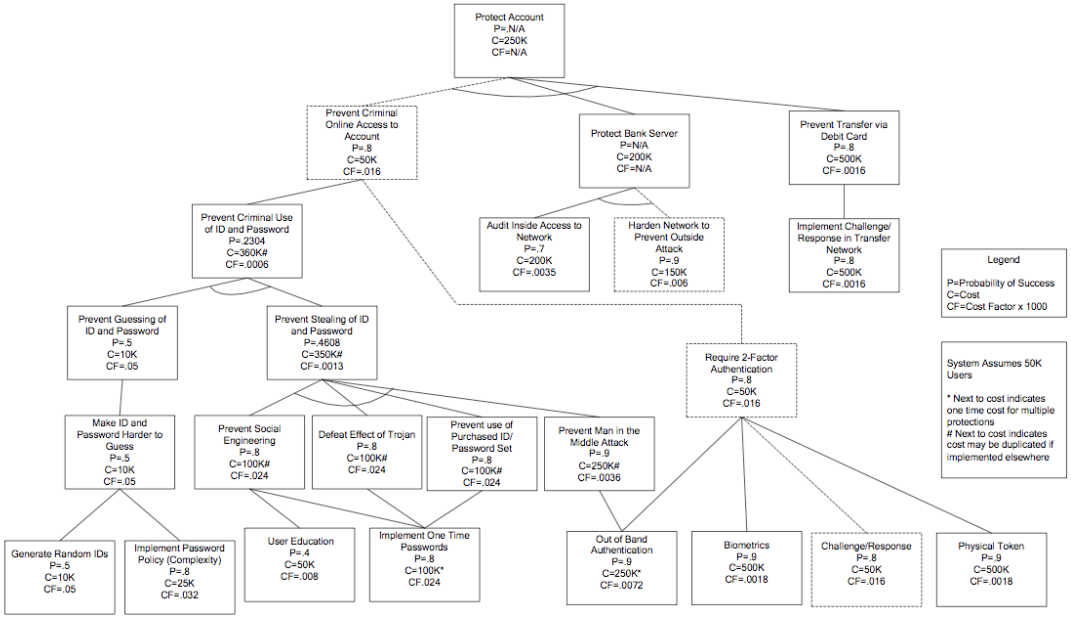


Figure 14 Online banking protection tree by Edge et al (2007)

As a conclusion of their practical work, Edge and et al (2007) define the utility of attack and protection trees to be fully realized in an environment of limited protection resources and further note that the technique aids the decision makers of a security system in choosing the most cost effective protections.

2.4. Scalability issues in Attack Graphs and Trees

Scalability is the main issue with the attack graphs (that also reflects to the attack trees). Ammann, Wijesekera and Kaushik (2002) state that with attack graphs the analysis pursuit most of the time becomes too large to be practical whereas with attack trees the same goal can be achieved with only the cost of monotonicity. Monotonicity means that no action an attacker takes interferes with the attacker's ability to take any other action which is a reasonable modeling assumption in most network analysis cases. This assumption states that the preconditions and the postconditions of the vulnerability are conjoined and the attacker will not backtrack.

Another approach to the scalability problem is put forward by Ingols, Lippmann and Piwowarski (2006) where the reachability matrix that represents the connectivity between arbitrary node pairs in a network is collapsed into smaller sub matrices and therefore the computational cost is reduced. Within this study the hosts that are treated identically by filtering devices are grouped so they have the same reachability within the subnet and cross different subnets of the network. Ingols, Lippmann and Piwowarski (2006) report results for a real operational network consisting of 252 hosts, 3777 ports and 8585 vulnerabilities to be studied on an attack graph of 8901 nodes and 23315 edges that can further be simplified. However this still presents a large and complicated task to perform.

In reference to this study Ou, Boyer and McQueen(2006) conclude that although research has made significant progress, no system has analyzed a network with large number of hosts and computation for most approaches scales poorly and would be impractical for networks with more than even a few hundred hosts.

In their study Vu, Khaw, Chen and Kuo (2008) propose a framework for network vulnerability analysis based on a vulnerability metric that enables the development of a more scalable algorithm to analyze and compute the desired security measure of the network without building the actual attack graph.

In some studies automated generation and analysis of attack graphs is proposed (Sheyner, Haines, Jha, Lippmann and Wing, 2002). Their technique is based upon symbolic model checking however it still presents a tedious effort in the model definition phase.

Noel and Jajodia (2004) proposed a graphical aggregation method to manage the attack graph complexity and further as Wang, Noel and Jajodia (2006) focused their effort on resolving the scalability issue of attack graphs. Their approach utilizes an algorithmic approach that focuses on initial conditions to come up with a method of search in the attack graph while avoiding logic loops.

In our TEOREM model we have decided to achieve an increase in the efficiency at the modeling and attack generation phase by prioritizing and focusing on the most critical IT assets by the identification of these assets through a methodology that embeds and puts the enterprise objectives at the forefront of the system modeling and IT asset definition phase. At the end the inclusion of this initial step acts as an inherent mechanism for the pruning of the attack tree that results in a computationally optimal width and depth for the tree that focuses on an outcome that is in synchronization with the enterprise objectives.

2.5. Enterprise Objective's integration

As was noted by Panda (2009) and depicted in Figure 15 most of the time the computing infrastructure is set up without IT staff having a clear understanding of the organization's mission or business objectives and it is not clear to them if critical and/or sensitive information is being adequately protected or not. Such a situation leads to absence of what can be termed as "organizational connect" between the technology and organizational objectives. Also most of the effort might be directed towards protecting relatively unimportant information. In order to resolve such issues operational or business units of the organization and the IT departments need to collaborate and communicate effectively to address the organization's mission or business-related needs. Within TEOREM we have the intention to devise a methodology that inherently addresses this problem and comes up with results that resolve missing "organizational connect".

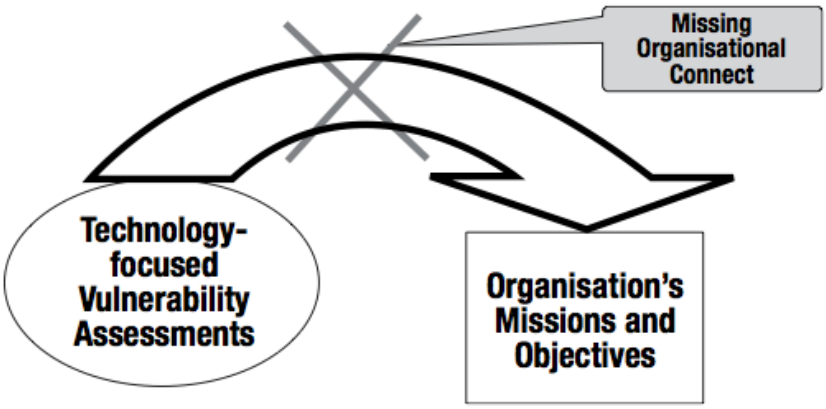


Figure 15 Missing "organizational connect"(Panda, 2009)

Similar arguments are shared by Brotby (2009) and he states that although technical security metrics have improved significantly in recent times they typically do not provide information useful or relevant to management beyond technical IT security. As an example knowing that there are a particular number of open vulnerabilities in the network is generally meaningless to senior management as it says nothing about the likelihood of exploitation, viable threats, potential impacts, or costs to remedy.

In order to start risk analysis on a system or infrastructure, first of all the relevant information assets within the system have to be defined. So a modeling or abstraction of the enterprise information and related assets is required. Hallberg, Hunstad and Peterson (2005) propose the below abstraction model in Figure 16.

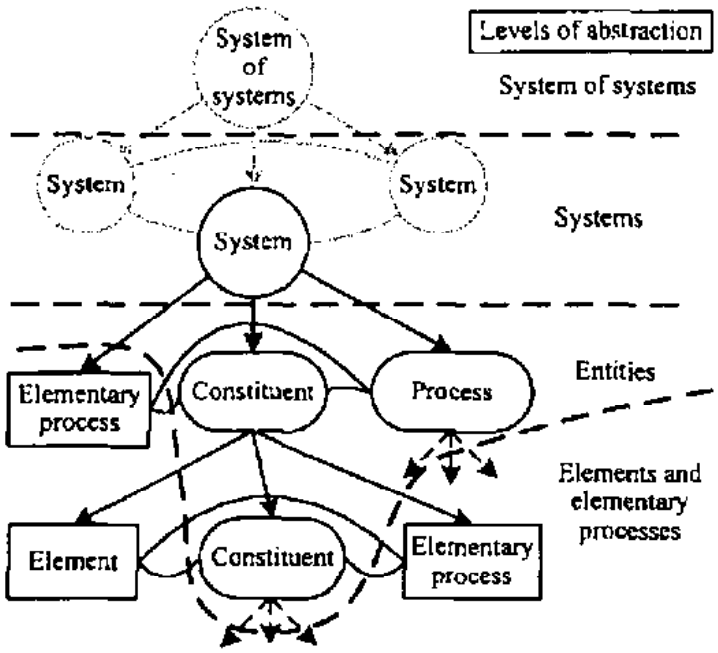


Figure 16 Abstraction levels in a system model by Hallberg et al (2005)

A similar layering has been proposed by Peterson (2004) and outlined in Figure 17. Within his model the entities are modeled as either traffic generators (computers or networks) or traffic mediators (firewalls, routers, proxies, hubs). Processes are not modeled in this approach and the relations are modeled as physical or logical relations.

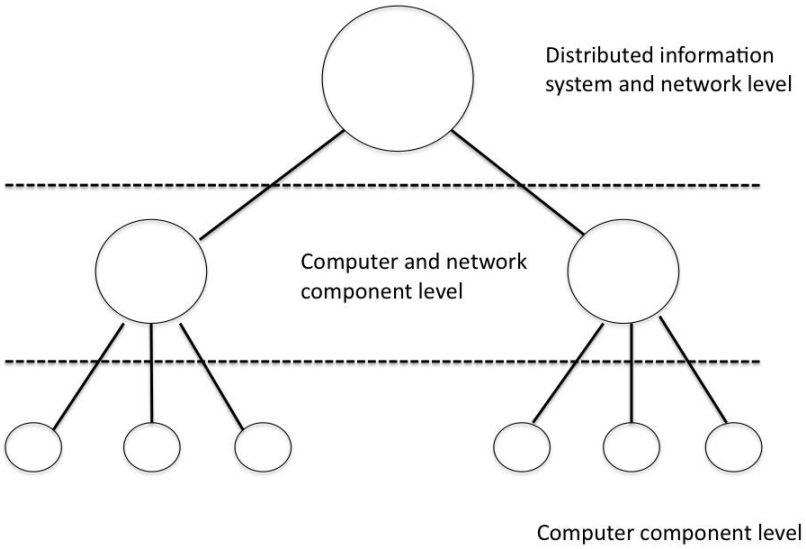


Figure 17 Levels of abstraction by Peterson (2004)

In another study by Naqvi and Riguidel (2006) the entities are defined as Security Enforcing Entities that directly contribute to satisfying the security objectives, Security Relevant Entities which perform any function necessary to support the enforcement of security and Security Irrelevant Entities. They are further classified as measurable, indirectly measurable and not measurable. From there they also use the CDG's. However their work is mostly useful and fit for purpose for telecommunication networks.

Another critical decision is the "boundary specification" as was pointed out by Bagheri and Ghorbani (2007). In their study focusing on the risk analysis in critical infrastructure systems they cover both the technical aspects of the system and also the socio-technical aspects of the system. Thus boundary definition becomes a crucial step. We also prefer to use this socio-technical viewpoint in the TEOREM so boundary definition will also be a critical step that will be addressed within the enterprise objective and asset definition phases. As long as the assessment effort is focused and limited to the enterprise objectives, this boundary definition objective will be inherently addressed.

Neubauer, Klemen and Biffl (2005) state that security (in itself) does not provide business value. Investment in an appropriate security level typically reduces the risk of loss of business value so the connection with business processes provides a common basis for the cost benefit valuation of security. Their view to IT security valuation is depicted in the Figure 18 below.

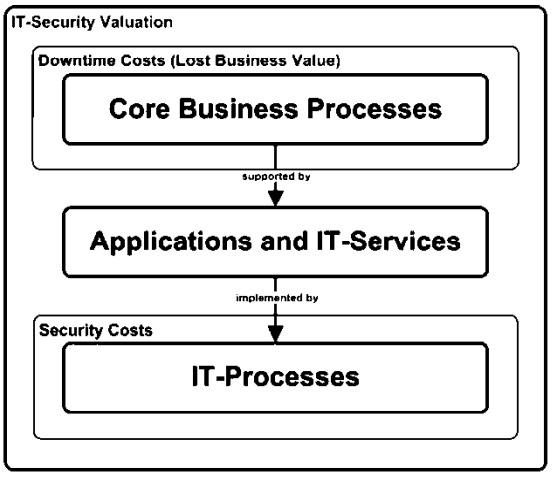


Figure 18 IT Security valuation by Neubauer at al (2005)

Neubauer, Klemen and Biffl (2005) further analyze the existence of the consideration for core business processes and the existence of a management view in different security models and frameworks. In the comparison outlined in Table 1 below;

- Consideration of the core business processes for valuation,
- Integration of methods for a cost benefit valuation,
- Management view on security in comparison to a pure technical view,
- Assessment and definition of security levels.

Table 1 Comparison of security models and frameworks by Neubuer et al (2005)

Criteria	1)	2)	3)	4)
Security Frameworks				
Cobit	-	-	+	+
GITBPM	-	-	-	+
ISO 17799:2000	-	-	+	+
Maturity Models				
SSE-CMM	-	-	-	+
ISPMG	-	-	-	+
SSM	-	-	-	+
SMM	-	-	-	+
Valuation Models				
ALE	-	+	-	-
SooHoo	-	+	-	-
CBA	-	+	-	-

Also within the OCTAVE approach by Software Engineering Institute, a necessity for matching the mission of the organization with the identification of assets is mentioned within OCTAVE's steps (Panda, 2009);

- Develop qualitative risk evaluation criteria based on operational risk tolerances
- Identify assets that are critical to the mission of the organization
- Identify vulnerabilities and threats to the critical assets
- Determine and evaluate potential consequences to the organization if threats are realized
- Initiate corrective actions to mitigate risks and create practice-based protection strategy

As was noted by Brotby (2009), defining objectives for security is critical to determining an approach to getting there, and it is also a requirement for developing meaningful metrics from both an operational standpoint and a strategic one. Without these objectives to guide the direction for information security and to

provide a reference point from which to measure management will remain inconsistent, haphazard and reactive. Metrics require objectives, and without defined objectives for an information security program it is not possible to develop useful metrics

Integration of business level perspectives to security metrics have been identified in various studies in addition to the work mentioned before by Clark, Dawkins and Hale (2005). Savola (2007) also underlines the importance of business level security metrics and suggests the usage of classical Goal/Question/Metric (GQM) method by Basili and Weiss (1984). In GQM the criteria for business success are identified as questions and finally the key criteria are broken down into measures that answer these questions. GQM method has also been proposed by Sultan, Nouaary and Lhadj (2008) for assessing the security risks of Software throughout the Software Development Lifecycle.

Breu, Oberperfler and Yautsiukhin(2008) comment on Clark, Dawkins and Hale's study (2005) as utilizing the number of existing vulnerabilities on the leaf nodes and treating them as risk measures (differing from a classical risk assessment methodology) during the risk aggregation phase. I also believe that an attack tree methodology will be a better fit for this pursuit as it takes into account the multiple layers and cascaded nature of attacks to information assets and processes. In fact Clark, Dawkins and Hale (2005) also refer to the application of fault tree analysis (precursor of attack trees as was outlined above) as a potential future path of study on their work and in their work in 2008 they use this approach.

In the further study by Clark, Singleton, Tyree and Hale (2008) a methodology is devised that attempts to integrate the enterprise goals with the risk assessment process. However in the identification of these, the enterprise goals are not clearly defined in their study. They criticize the pre assessment phase in the NSA's InfoSec Assessment Methodology as its usage of management interviews and review of mission statements that do not provide a formal relationship between

assets and objectives. They also refer and criticize the Critical Success Factors method and its usage in the information security field by Caralli (2004), as it does not provide a relationship between the critical success factors and the network assets that fulfill them. Critical success factors as outlined by Rockart (1979) are essential for gaining and maintaining competitive advantage. These describe the areas in which good results ensure success in competition and poor results will definitely fight against the end results of the company's operation. In the definition of these factors industry characteristics, competitive position, general environment and organization developments are decisive factors.

However there are strong counter agreements to the Critical Success Factor method. Within the work by Amit and Schoemaker (1993) it was stated that the consideration of the industry as the primary unit of analysis in this method is not adequate as firms operate on their own and from their own perspectives. Also the empirical analysis in critical success factors is ex post whereas the managers make resource deployment decisions ex ante which involves uncertainty, complexity and organizational conflict. Most importantly if all firms score high on these critical success factors these factors will cease their importance as the key success factors.

Also these success factors approach has been criticized by Ghemawat (1991) as lacking identification as there may be many success factors making it hard to focus on some of these, concreteness as there is ambiguity about the causal processes that tie the firm's success factors to its performance, and generality as the to be success factors must be undervalued, and finally necessity as the success factor method fails to account for the dynamic aspects of strategy. So we believe that although Clark et al's (2008) attempt in integrating enterprise goals with the risk assessment process is a right move, they do not propose an integrated solution to for the practitioners to execute this critical step and the details of this step is not clearly defined in their methodology.

For this most critical step of Enterprise Objective Fusing/Integrating to the IT security vulnerability measurements we decided to use tools from the discipline of management in TEOREM. These processes will be utilizing the tools borrowed from the discipline of management theory based on the Resource Based View (RBV) of a company.

2.6. Resource Based View of the company

In the Resource Based View (RBV) of a company as was outlined in the works of Wernerfelt (1984), Peteraf (1993) and Barney (1991), firms are collections of tangible and intangible assets combined with capabilities to utilize these assets to finally develop competencies that result in competitive advantage. In a formula by Collins and Montgomery (1995);

(Tangible Assets + Intangible Assets) X Capabilities = Competencies => Competitive Advantages

In this definition the assets refer to factors of production a firm may use to come up with products and/or services. These include tangible assets like property and equipment and may also include intangible assets like a brand name, corporate culture, organization structure etc. Capabilities of a company define the skills the firm needs to take full advantage of these assets. Competencies and finally competitive advantages are a direct outcome of these items. Competencies (Teece et al., 1997) are developed when combinations of resources are applied in conjunction to come up with organizational abilities. So a competency can be defined as a firm's ability to deploy resources in combination to create a capacity for achieving a desired objective. These are firms' distinct abilities that help firms achieve superior performance within competitive settings.

Wernerfelt (1984) states that;

- Looking at firms in terms of their resources leads to different immediate insights than the traditional product perspective.
- One can identify types of resources which can lead to high profits. Analogous to entry barriers, these are associated with resource position barriers.
- Strategy for a bigger firm involves striking a balance between the exploitation of existing resources and the development of new ones.

Further Wernerfelt (1984) states that, a resource is meant to be anything which could be thought as a strength or weakness of a given firm. A firm's resources at a given time can be defined as the tangible and intangible assets that are semi-permanent ties to the firm like the brand name, in-house knowledge of technology, employment of skilled personnel, trade contacts, machinery, efficient procedures, and capital. Wernerfelt (1984) summarizes these in a resource product matrix as in Table 2;

Table 2 Resource-product matrix (Wernerfelt, 1984)

		Resources				
		I	II	III	IV	V
Markets	A	X				X
	B	X	X			
	C		X		X	
	D			X		X

Some of the resources in the company consist of knowhow that can be traded, financial or physical assets, human capital. They are information based tangible or intangible processes that are firm specific and are developed over time (Amit and

Schoemaker, 1993). Within this analysis by focusing on the firm as the relevant unit of analysis, managers are concerned with the creation of tangible and intangible resources and capabilities whose economic returns are appropriable by the firm. By using these scarce, durable, not easily traded and difficult resources enables a firm to earn economic rents so using the resource perspective the value of a firm' strategic assets extends beyond their contribution to the production process. Below in Figure 19 is a chart that outlines the desired characteristics of the firm's resources (Amit and Schoemaker, 1993).

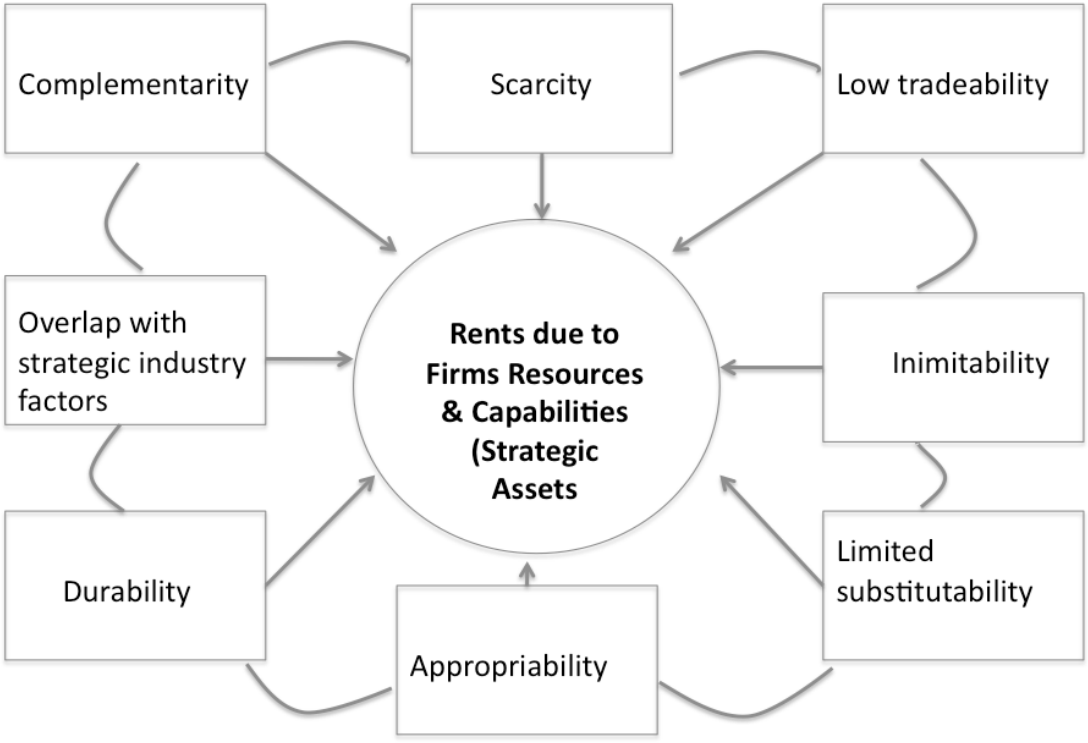


Figure 19 Desired characteristics of firm's resources by Amit and Schoemaker (1993)

In his seminal work Barney (1991) states that there are four indicators of the potential of firm resources to generate sustained competitive advantage and these are the value, rareness, (in)imitability and (non)substitutability, this criteria is

called as the VRIN (value, rareness, inimitability and nonsubstitutability) criteria. These resources can be physical resources like the physical technology used in a firm, firm's plant and equipment, geographic location and its access to raw materials, or the human capital resources like the training, experience, judgment, intelligence, relationships and insights of managers and workers in a firm, or the organizational capital resources like the firm's formal reporting structure, its planning system, controlling and coordinating systems. In addition to that there exists resources which are not tangible. Barney (1991) further refines the four indicators as follows;

Value: Firm resources are valuable when they enable the firm to implement strategies that improve its efficiency and effectiveness, and only then they can be considered as resources.

Rareness: A firm enjoys a competitive advantage only if the same advantage is not shared by another firm, so the rarity of the resource is a decisive criteria for it to be accepted as a resource.

Imitability: In order to offer a sustainable advantage a resource must be harder to imitate by the competition. This low imitability limits also lowers the mobility or increases the time to copy for the resource.

Non-Substitutability: Resources that are critical must not have equivalent resources (with lower rareness or imitability) that can substitute them. Existence of such substitutes voids the importance that the particular resource presents.

In order to analyze the outcome of these 4 criteria we can refer to the decision matrix outlined in Table 3 below;

Table 3 Analytical framework of Resource Based View criteria (Cunha, 2007)

Valuable?	Rare?	Difficult to Imitate?	Difficult to substitute?	Competitive Position
No	No	No	No	Competitive disadvantage
Yes	No	No	Indifferent	Competitive parity
Yes	Yes	No	Indifferent	Temporary competitive advantage
Yes	Yes	Yes	Yes	Sustainable competitive advantage

Although there are numerous studies that discuss the underlying reasons behind the heterogeneity of resources between the companies like the study by Helfat and Peteraf (2003) as we focus on the end result (the resources that exist within a company at the time of our security assessment) we do not discuss these in detail. As was noted by Mahoney and Pandian (1991) the distinctive competence is a function of the resources which a firm possesses at any point in time and usually for the information security assessments that snapshot of time is the focal point.

Recently Resource Based View analysis focusing on the IT sector have been performed by Meirelles, Basso and Pace (2008) and also Wagner (2006) has done research on the impact of IT on firm success by linking the Resource Based View with the IT Infrastructure Library. Another interesting research is performed by Jarvenoaa and Leidner (1998) to challenge the basic assumptions of Resource Based View, attractive local markets, stable environments and the limitation of management on sustained advantage. In doing so they have applied RBV analysis to an information company in Mexico and checked and validated the viability of RBV within an emerging market environment within which local market was not that attractive and environment was unstable.

So it can be said that in order to reach the Enterprise Objectives, the Resources that are identified by the Resource Based View approach to a company are essential. So if we focus on these resources in the end we will be focusing on the Enterprise Objectives and if we identify the information assets relevant to these resources we will be prioritizing and limiting our threat assessment effort in the right and relevant direction. So our intention is to utilize the Resource Based View to

identify, prioritize and limit the number of IT assets that are crucial for the completion of enterprise goals and objectives and further limit our security risk assessment efforts towards these.

Jaquith (2007) define a good metric as;

- Consistently measured, without subjective criteria,
- Resource optimal, preferably in an automated way,
- Expressed as a cardinal number of percentage, not with qualitative labels,
- Expressed using at least one unit of measure, such as defects, hours or dollars,
- Contextually specific, relevant enough to decision makers so that they can take action.

We believe that within TEOREM most of these points are addressed and specifically the optimal resource requirement, automated nature and context specificity within the usage of Attack Trees embedded in a RBV framework.

Herrmann (2007) claims that one factor that contributed to the delay in the development of security metrics is the confidentiality, integrity and availability model (which in itself was a simplistic model). It ignores the extensive interaction among all four security engineering domains, physical, personnel, IT and operational security. So it cannot form the basis for a holistic viewpoint. Utilizing the Resource Based View within the enterprise objective definition phase, this holistic approach is inherently present within TEOREM.

CHAPTER 3

TEOREM – TREE BASED ENTERPRISE OBJECTIVES RISK EVALUATION METHOD AND METRIC

3.1. Main idea of TEOREM

Within this design science based research the main artifact is a method, which utilizes Resource Based View (RBV) model of enterprises in the fundamental phases of the method and is used to identify the resources essential for an enterprise's success in line with objectives. The method further maps these resources and thus the enterprise objectives with the information assets domain. Resources and related assets are analyzed from the information security threats perspective. Resource-based view of an enterprise identifies enterprises as collections of tangible and intangible resources combined with capabilities to utilize these assets to finally develop competencies that result in competitive advantage. Until now it has not been used within the context of information security risk tools and methodologies.

System security risks are of a complicated nature which can only be evaluated by considering a complex combination of possible consequences. Attack trees are well

suited and frequently used for this pursuit, so that attack tree modeling are utilized in the information asset and threat modeling stage as described herein. A purpose of the attack tree is to define and analyze possible attacks on a system in a structured way that is modeled within a tree structure including a nodal hierarchy that allows the decomposition and analysis of an attack within a number of attack steps.

Thus, the inclusion of the enterprise objectives enables results to be determined that will be inherently relevant to the decision making and execution steps of management. Identified resources through the resource based view constitute the root nodes of the attack tree and the related information assets and the steps of the threat scenario against these form the leaves of the attack tree. In addition, the techniques described will increase the efficiency of the method against the scalability issues, with using the attack trees at the modeling and attack generation phases by prioritizing and focusing on the most critical information assets by the identification of these assets through a methodology that embeds and puts the enterprise objectives at the forefront of the system modeling and information asset definition phases.

Therefore, the usage of the resource-based view enables integration of enterprise objectives with vulnerabilities presents useful results for the management and resolves the scalability issues inherent with the attack tree modeling of information security threats.

An enterprise under discussion can be any organization such as a business, a university, a non-profit organization and so forth utilizing information assets. Enterprise objectives are either defined within mission statements and/or goals of an organization or can be compiled through discussions with the top level management of the company. Enterprise resources may be identified, through a rigorous resource-based modeling of the enterprise and enterprise resources are based upon the relevant information assets that are identified. After the

identification of the enterprise objectives, the enterprise resources, the information assets and a mapping of these elements to each other, a refined list and model is achieved that can be focused to determine information security.

Enterprise objectives such as missions and goals are also compiled and a team that includes an enterprise's top management and functional managers (e.g., sales, marketing, finance, technical, logistics and so forth) determine a list of tangible and intangible enterprise resources, which are stored into a system to determine the risk. Usually the enterprise objectives take the form of mid- to long-term measurable goals that set the direction for the enterprise as a whole. Examples of such enterprise objectives can be the achievement of X % revenue growth within the next two quarters, obtaining Y % market share within the end of year Z, cultivation of a learning organization culture, achieving six sigma quality levels in three years, leading the innovative position within the industry in research and development. Afterwards, a team of top management and functional managers define the enterprise resources. Such resources may include all assets, capabilities, organizational processes, brands, information and knowledge base that the company owns, which, for example, may be in the form of tangible or intangible entities. Some examples for the resources may cover; brand names, in-house knowledge of technology, skilled human resources, patents, proprietary technologies, efficient procedures, specialized machinery.

A list of enterprise information assets is defined by the information systems team in the enterprise and stored in the system as well. Identified resources are mapped with the identified objectives to form a limited list of resources that are mapped with the enterprise objectives. Afterwards the identified objectives are matched with the identified resources that are relevant for the successful achievement of the objectives. Such resources may include but are not limited to; servers (database, Internet, e-business, mail, customer relationship management, enterprise resource planning etc.), personal computers, thin clients, mobile computing platforms, network infrastructure (such as routers, switches, bridges, hubs), smartcard

systems, RFID systems, point of sale systems, automated teller machines, information security appliances (firewalls, intrusion detection/prevention systems, antivirus tools etc.), private branch exchange telephony systems, closed circuit TV systems, data storage infrastructure, and so forth.

Filtered list of enterprise resources are mapped with the relevant information assets from the identified list of assets defined in the previous stages to form a mapped list of information assets with the critical resources. Identified enterprise resources are matched with the identified assets that are relevant for the proper functioning of the resource. As an example if "leading the innovative position within the industry in research and development" was the enterprise objective at hand than the related enterprise resources to be mapped could be, for example, patents owned by the enterprise, proprietary technologies, skilled human resources, and specialized machinery (lab tools). In the same example the information about the "proprietary technologies" reside within the knowledge database of the research and development team or in the computers of the team members (e.g. in the form of software code). Also the "specialized machinery" resource can be a special lab tool used by the R&D team with connections to the R&D intranet. So the related information system assets will be all the computers, servers and network components within the R&D intranet and with direct connections to this intranet as the compromise (e.g., in the form of a security breach or an availability problem such as the downtime of the specialized lab tool) of these resources leads to the compromise of an enterprise resource (proprietary technology or specialized machinery) which directly affects an enterprise objective (leading the innovative position within the industry in research and development).

A value, rareness, inimitability, non-substitutability (VRIN) criteria test is then used to refine and filter the enterprise resources to include enterprise resources that are relevant to the proper and successful functioning of the enterprise. The VRIN criteria are based upon the resource-based view of the enterprise and define differentiating, competitive and advantageous resources of the enterprise.

For each enterprise resource, the enterprise resource is evaluated against a value criterion and this value criterion defines that an enterprise's resources are valuable if they enable the enterprise to implement strategies that improve its efficiency and effectiveness. Value criterion can be a Boolean and/or qualitative criterion that has a PASS/FAIL or COMPLIANT/NON-COMPLIANT value. Thus, the enterprise resources that fail the value criterion are discarded.

Enterprise resources that pass the value criterion are further evaluated against a rareness criterion within which the rareness criterion from the resource-based view paradigm indicates that an enterprise has a competitive advantage if the same advantage is not shared by another enterprise. This criterion may also have a Boolean and/or qualitative criterion that has a PASS/FAIL or COMPLIANT/NON-COMPLIANT value. Thus, the rarity of the enterprise resource is a decisive criterion for it to be accepted. Thus, the enterprise resources that fail the rareness criterion are discarded.

Enterprise resources that pass the rareness criterion are further evaluated against an inimitability criterion and this criterion indicates that in order to offer a sustainable advantage an enterprise resource is harder for a competing enterprise to imitate. For example, a low inimitability limit also lowers the mobility or increases the time for the enterprise resource to be copied and the enterprise resources that fail the inimitability criterion are discarded.

Finally the enterprise resources that pass the inimitability criterion are further evaluated against a non-substitutability criterion which indicates based upon the resource-based view thinking that enterprise resources that are critical do not have equivalent enterprise resources (e.g., with a lower rareness criterion value or an inimitability criterion value) that can be substituted for them. For example, existence of such substitute enterprise resources voids the importance that the particular enterprise resource presents. The enterprise resources that fail the non-

substitutability criterion are discarded and the enterprise resources that pass the non-substitutability criterion form the filtered/refined list of enterprise resources.

All the enterprise resources that are refined and filtered in the VRIN analysis are mapped with the information assets defined in the previous steps to form a mapped list of information assets with the enterprise resources and upon which the outcome of this process forms the basis for risk analysis. Threats and threat scenarios that include a succession of serial and/or parallel steps of hostile moves that may jeopardize a specific enterprise resource are modeled using an attack tree and in forming the attack tree, the enterprise resources that successfully pass previous steps are used as the root nodes of the attack trees. Attack steps against the information assets that are relevant for this resource form the lower layers form the leaves of the tree. For the purpose of quantitative analysis numerical values are assigned to the leaf nodes such as, for example, a probability, a cost, and/or an impact of the related attack step.

Using the values from this process and the AND/OR logic outlined above, the attack scenario steps values are determined. For the resultant impact, probability and risk level of an attack or series of attacks against the enterprise resources, a resultant risk value is determined. For each layer in the attack tree, it is determined if more than one threat act is required and it is determined if either of the threat acts suffice. A logical AND step is used if more than one attacker moves in parallel and a logical OR is utilized if the attacker can successfully pass a certain layer within the performance of either one of the attack steps.

By using the successive mapping steps and using the resource filtering of resource based view criteria, an essential list of resources and related information assets are identified. Thus, using this limited (but relevant) list of assets/resources to form the attack trees, the scalability issue of the attack tree analysis is overcome. Also the list of resources/assets pertain resources/assets that are relevant to the fulfillment of

enterprise objectives and the results of the analysis is therefore beneficial not only in the technical domain but also for managerial decision making.

Appendix B includes the patent application documents for the US Patent and Trademark Office, with a focus on the application and execution of TEOREM with a step-by-step approach. Also this appendix entails a visual representation of the stages and application of the method.

3.2. Steps of TEOREM

In performing an IT security risk analysis on an enterprise scale utilizing TEOREM the step by step application will be as follows;

Enterprise Objective and Resources definition: Utilizing the Resource Based View of a company defined in previous sections, we will come up with an effective list of business resources that matter most for an enterprise's success or failure in line with its objectives. In doing so;

1) Enterprise's missions, goals and objectives are compiled from the top management of the company as the main input. Most of the time these mission, goal and objective definitions are readily available within the organizations as part of corporate policy documents. Such definitions are the outcome of separate studies that have been performed within the organization together with the participation of the organization's staff and sometimes with respective consultants on those areas. In some other instances (especially for small to medium sized enterprises) these goals and objectives must be identified within the TEOREM process. In such cases the management team of the organization under discussion intends to come up with a list entailing these objectives.

2) A team is formed consisting of members of the organization's top management and also the managers of the functional departments within

the organization (finance, manufacturing, marketing, sales, technical, logistics, human resources). Usually it is advisable to assign and have a "champion" within the enterprise that leads the effort and support and commitment from the management level is a prerequisite for the success of the effort. Forming a team as was outlined above both addresses the managerial commitment and also serves as a melting pot within which the communication among all the stakeholders of the process is easily performed.

3) This team comes up with a list of enterprise resources like physical, financial, human capital, knowledge capital (patents, processes), and intangible (brand name etc.) resources.

   One of the important challenges Resource Based View researcher faces is the identification of resources. Competencies (Prahalad and Hamel, 1990), skills (Grant, 1991), strategic assets (Amit and Schoemaker, 1993) have been identified within the works of different researchers. However the attendance of managers from all stakeholder departments and also the existence of executive management within the team ensure the functioning of this team and its efficiency in identifying the resources with a multi-faceted approach.

4) A mapping is performed between the enterprise objectives that were assembled at step 1 and the resources identified at step 3. Although this step may initially sound as a mechanical process, it requires the in depth knowledge of the inner workings of the enterprise and its processes. Existence of the relevant staff as team members ensures the proper execution of this critical step.

5) Resources are later the subject of a VRIN (value, rareness, inimitability and nonsubstitutability) criteria test to be further refined and limited. Proper

care must be exercised at this step as most of the power of TEOREM is inherently witnessed within this step. Pruning of the final attack tree is a direct consequence of the VRIN filtering applied at this stage and also the relevance (from the match with enterprise resources viewpoint) of the outcome stems from the proper application of VRIN criteria.

6) Resultant resource pool outlines the resources that are critical for the achievement of Enterprise Objectives. This list of resources form the input for the later stages of TEOREM

Information assets identification: Utilizing the resource pool list identified in the previous section the enterprise information assets are selected and mapped to the enterprise resources. In doing so;

1) Another team is formed with the members of functional departments and the members of the IT team within the organization. Actually this team is an expanded version of the previous team with the IT team members of the organization and also the attendance of the top management is not required to the team. However ongoing management commitment to the process is essential for its success.

2) Team takes the enterprise resources (tied to the Enterprise Objectives) identified in the previous section as the input. Mentioned list consists of enterprise resources that have passed (and thus being filtered by) the VRIN criteria.

3) Team identifies the information assets required for the proper functioning of each and every enterprise resource identified in the previous section, in depth knowledge of the enterprise IT assets is crucial in this step and that is the reason IT team members are present within the team at this stage.

Some researchers have focused on the information systems assets identification. Ross et al. (1996) divided information systems assets into three categories, human assets (technical skills, innovation skills, business understanding, and problem-solving capacity), technology assets (physical IT assets like hardware, software, networks, technical platforms, databases, architectures, standards) and relationship assets (partnerships, client relationships). IT processes deemed as assets are planning ability, cost effective operations and support and fast delivery. So any hindrance and negative impact to the above outlined assets and processes have to be taken in to account within this step.

Attack Tree formulation: After the enterprise objective definition, enterprise resource identification and the information asset selection phases, an attack tree is formulated taking into account the Enterprise Objectives and thus the enterprise resources in the form of assets, processes, confidential information (either from patent or privacy perspectives), (taking into account the Enterprise Objectives) as the root nodes and the related information assets as the branch nodes. Within this step additionally the attacker profiling can be implemented. Commercially available tools exist for this purpose such as the SecurITree by the Ameneza Technologies Ltd. Using such tools further optimizations to the attack trees like pruning can be performed, and the attack agents can further be profiled according to their resource availability, skill level and counter threat avoidance levels (utility functions). Essentially this is a technically oriented step within which the proper staff members that are literate in attack tree formation work in unison with the IT team members to come up with the resultant attack tree. In Figure 20 is a work in progress attack tree.

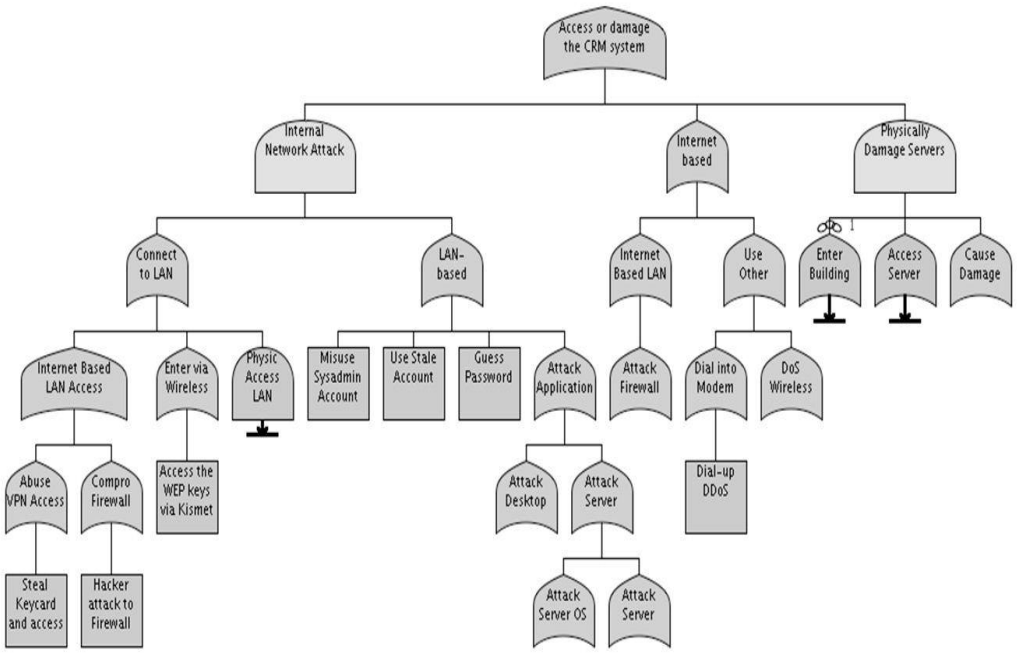


Figure 20 Work in progress Attack Tree

Analysis: In the analysis phase, different measurements can be performed as checking the feasibility of certain attacks, the costs involved, prioritization of certain exposures etc. Different metrics can be devised using the attack tree approaches, for the calculation of these metrics within the traversal of the tree, the formulation outlined in Table 4 by Edge et al. (2006) is utilized;

Table 4 Rule set to propagate metrics up tree (Edge et al , 2006)

	AND	OR
Probability	$\prod_{i=1}^{n} prob_i$	$1-\prod_{i=1}^{n}(1-prob_i)$
Cost	$\sum_{i=1}^{n} cost_i$	$\frac{\sum_{i=1}^{n} prob_i \times cost_i}{\sum_{i=1}^{n} prob_i}$
Impact	$\frac{10^n - \prod_{i=1}^{n}(10-impact_i)}{10^{(n-1)}}$	$Max_{i=1}^{n} impact_i$

$prob \in (0,1], cost \in (0,\infty), impact \in [1,10], n = \#$ of child nodes

Also during the process of assigning numerical values to different impact ratings Edge et al. (2006) proposed a table based definition listed in Table 5 below.

Table 5 Impact definitions and numerical mapping by Edge et al (2006)

Numerical Range	Impact Definition
1-3	Minor impact to system. May be a nuisance but is easily detected and/or repaired
4-6	Moderate impact to system. Confidentiality, integrity, and/or availability of system affected. Requires non-trivial effort to detect and/or repair.
7-9	Severe impact to system. Significant damage results to system. Considerable effort required to detect and/or repair damage.
10	System completely compromised, inoperable, or destroyed

So it can be said that within the application of TEOREM the focus moves from the macro level enterprise objectives down to the detailed analysis of individual vulnerabilities and threat identification. In the following Figure 21 a higher level look to the TEOREM can be performed:

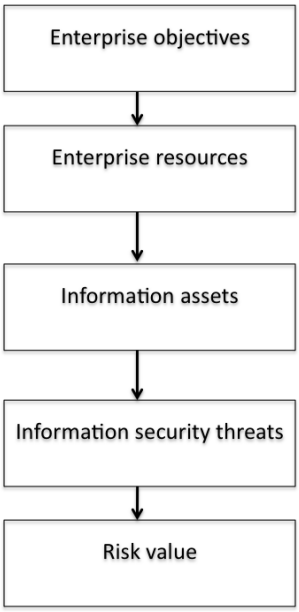


Figure 21 A macro level outline of TEOREM's steps

Appendix B includes the patent application documents to the US Patent and Trademark Office and a step-by-step execution of the devised method is also outlined within this document

CHAPTER 4

RESULTS AND DISCUSSION

In line with the Design Science Research based approach taken, the ultimate outcome of this study was the artifact in the form of an information security risk assessment method. In order to test the effectiveness of TEOREM within a real life environment, the application of the method within a real life setting was essential. In parallel to that to test the secondary objectives of the method we applied a hybrid approach utilizing both a quantitative experiment approach and also a case study research approach. Although the fundamental outcome of this design science based research is the artifact in the form of a method (utilized and verified within a real life enterprise setting) the additional dual mechanism of quantitative experiment and qualitative case study was performed due to the fact that TEOREM also attends to address two additional objectives;

- To improve the scalability issues witnessed within attack graph and attack tree methodologies with an increase in efficiency so that the metric and the risk assessment process becomes applicable for small and medium enterprises and the task becomes manageable for large enterprises.

- To ensure that the outcome serves the needs of the managerial community as well as the technical community. This goal is achieved by the integration of enterprise goals and objectives to the process.

In the following sections the selection of appropriate research methodologies for this pursuit will be outlined.

4.1. Case study research

Case study research is one of the several ways of doing social science research together with experiments, surveys, histories and economic and epidemiologic research (Yin, 2009). Each of these approaches have different strengths and weaknesses, but specifically case study research is one of the most common qualitative research approaches also in the domain of information systems (Myers, 1997). As was noted by Yin (2009) although there is no formula for the usage of case study research the choice depends in large part on the research question and the more that the questions seek to explain some present circumstance the more that the case study method will be relevant. Also the method is relevant the more that the questions require an extensive and in-depth description of social phenomenon. Yin (2009) also highlights that the case study method allows investigators to retain the holistic and meaningful characteristics of real-life events such as individual life cycles, small group behavior, organizational and managerial processes. This is further underlined by Yin (2009) as a “how” or “why” question that is asked about;

- A contemporary set of events,
- Over which the investigator has little or no control.

In addition to that Yin (2009) defines the scope of a case study as an empirical inquiry that;

- Investigates a contemporary phenomenon in depth and within its real life context, especially when,
- The boundaries between phenomenon and context are not clearly evident.

And also notes that the case study inquiry;

- Copes with the technically distinctive situation in which there will be many more variables of interest than data points, and as one result,
- Relies on multiple sources of evidence, with data needing to converge in a triangulating fashion, and as another result,
- Benefits from the prior development of theoretical propositions to guide data collection and analysis.

Taking into account all these findings we have decided to use the case study research method to observe and verify the effectiveness of TEOREM in integrating the enterprise goals and objectives to the metric and the risk assessment process. As was discussed before this trait of TEOREM was intended for the method and metric to come up with end results that are useful for the management community as well as the technical community. We believed that a case study based method will test the validity of this aim.

So in order to achieve these goals and come up with a quality research design we have decided to utilize a “multiple case design” within which both “interviews” and “direct observation” would be performed to triangulate the research findings and to cross check the data achieved.

4.2. Quantitative experiment

Within the application of the case study research methodology we have intended to apply “mixed method design” as one of the intended outcomes from the TEOREM was a quantitative end result, namely improving the scalability problems with the

attack graph and attack tree methods. So in order to address this objective we had to check the validity of TEOREM's efficiency increase in attack tree modeling. For this purpose a series of TEOREM applications have to be performed by a sample of individuals within the same operational environment and then the results that is the comparison of TEOREM enabled process timings with the TEOREM-less application must be compared and analyzed for statistical significance.

4.3. Research design

In order to apply our intended mixed method approach we have chosen a technology company and both for case study method with multiple case analysis and also for the experiment, a division within the company has been analyzed. Selection of a department instead of the whole company was necessitated for practical applicability reasons. Company is active in the telecommunications sector with branch offices at 4 locations.

Six teams (of three to four employees) performed IT security assessments on this same department with and without using TEOREM and the timing results of these experiments were recorded and further analyzed from the statistical significance viewpoint. Teams were briefed prior to the experiments and the experiment times were not included in the analysis. Team members were not IT security professionals but all of them were technology literate. As the statistical methodology the "inference about the difference between the means of two populations: matched samples" approach was used. Also we have benefited from the matched sample approach as the same teams performed the two separate test scenarios.

In parallel to that a case study methodology was applied using both "interviews" with the management team, and also by doing "direct observation" during these multiple cases.

4.4. Quantitative analysis

While performing the case study, a quantitative experiment and statistical analysis was also performed, as one of the intended outcomes from the proposed method was a quantitative end result, namely improving the scalability problems with the attack graph and attack tree methods. So in order to address this objective, the validity of TEOREM's efficiency increase in attack tree modelling had to be verified. For this purpose a series of real life applications of the method were performed by a group of teams within the same operational environment and then the results (that is the comparison of TEOREM enabled process timings with the straightforward application of attack trees) was compared and analysed for statistical significance.

Multiple assessment teams (of three to four people each) performed the IT security assessments on this same department with and without using the proposed method (the order of methods was different for half of the individuals) and the timing results of these experiments were recorded to be further analysed from the statistical significance viewpoint. As the statistical method the "inference about the difference between the means of two populations: matched samples" approach was used. Also the matched sample approach was beneficial as the same teams were performing the two separate test scenarios and sample bias was avoided.

In Table 6 the execution times of the assessment teams for both risk assessment methods are listed. μD denotes mean of the difference between the completion times for the two methods and the null and alternative hypothesis are;

$H0: \mu d = 0$

$Ha: \mu d \neq 0$

$\alpha = .01$ with 5 degrees of freedom, so $t_{.005} = 4.032$ where

$d = \Sigma di/n$ and $t=(d- \mu d)/(sd /\sqrt{n})$,

Taking into account the data within Table 6, H0 is rejected as

sd = 0.816 and t = 7.0 > 4.032.

So we can state that using TEOREM method, a statistically significant (with α =.01) efficiency level is reached against the straightforward application of attack tree modeling.

Table 6 Risk assessment method execution times (in hours)

Team	Direct implementation (hrs)	TEOREM implementation (hrs)
1	8.0	5.0
2	6.0	4.0
3	7.0	6.0
4	9.0	6.0
5	8.0	5.0
6	9.0	7.0

4.5. Case study research

A "multiple case design" within which both "interviews" and "direct observation" took place was performed to triangulate the research findings and to cross check the data achieved. A medium scale technology company was analysed from an information security assessment viewpoint using the proposed method. Multiple assessment teams (all with technical backgrounds) performed the IT security assessments on this same department with and without using the proposed method (the order of methods was different for half of the teams) and in the case study research phase the authors also participated the process for observation. In parallel to that upon the conclusion of the risk evaluation the reports were shared with the management team within the company and "interviews" were performed to analyse the managerial relevance of the analysis outcome.

So a mixed (hybrid) case study research methodology was applied for triangulation purposes via interviews with the management team and in parallel with direct

observation during and after the execution of these multiple cases. Direct observation that has been performed can also be considered as action research as the authors were partially involved in the execution of the case study (as supervisors).

Interviews were performed with board members, executive managers and department managers and a semi-structured, questionnaire based but open-ended format was utilized, questionnaire forms included 12 questions with additional open ended discussions that lasted in total around 45 minutes for each manager. Questionnaire format included questions with 5 degrees of ordinal variables as answers. Questions from this questionnaire are listed within Appendix C. During the interviews two main issues were investigated based upon the two versions of risk assessment reports (plain attack tree application versus TEOREM enabled version):

- If the proposed method outcomes came up with results that are more useful/beneficial for the managerial decision making processes (2/3 of all questions),

- If the enterprise asset coverage of the proposed method's outcomes is more holistic (including intangible assets as well) compared to the straightforward attack tree implementations (1/3 of all questions).

Results from the case study questionnaire are outlined within Figure 22 for both TEOREM enabled and plain implementation of attack trees and out of the 5 degree ordinal scale the higher score averages are positive indicators for the proficiency within that specific domain.

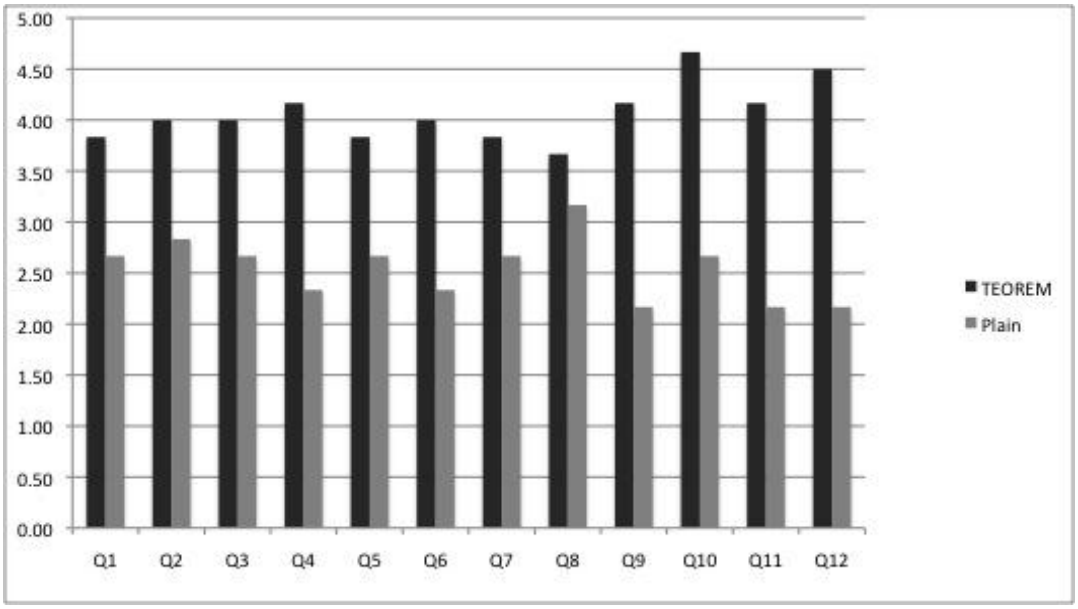


Figure 22 Case study questionnaire results for TEOREM and plain attack tree

In addition to the questionnaire findings, both within the open ended discussion phase of the interviews and also within the participatory observation stages of the case study research the authors witnessed the effectiveness of the TEOREM method in addressing the needs and expectations of the management audience with outcomes that are beneficial to their decision making processes.

As a result of the interviews and the direct observations during the implementation it can be inferred that;

- TEOREM comes up with results/findings that the management perceives better suited for further decision making like mitigation decisions, prioritization and resource allocation,
- Intangible assets are included within the scope of TEOREM enabled assessments whereas straightforward implementations of attack trees came up with results that are more focused on technical information assets.

(However for the individuals that performed the TEOREM approach as the first run, intangible assets were also included in the second straightforward application. So a learning/enlightenment effect prevailed for the second run),

- Although it has not been predicted beforehand, the involvement of the management during the enterprise objective definition phase in TEOREM seems to leave a lasting positive attitude against TEOREM's results. This may also be perceived as a bias.

CHAPTER 6

CONCLUSION

Within this study an extensive survey of the existing IT security risk evaluation methods and metrics have been performed and the current state of research in IT security risk evaluation has been digested and their powers and limitations are analyzed. In the current state there exist a limited number of alternative methods that take the Enterprise Objectives into account within their frameworks and integrate these to the methods and metrics. Also it has been observed that utilization of component dependency based approaches, be it component dependency graphs (CDG), attack graphs or attack trees, serve well to the purpose of analyzing the multi layered and cascaded nature of current IT attack scenarios. So we have decided to devise an IT security risk evaluation method and metric that utilizes attack trees in its operation. In addition to that we have decided to embed the enterprise's business level objectives into the process so that the outcome would serve the needs of the management in addition to the technical staff. Also this approach improves the issue of scalability inherent in attack graph and attack tree based methodologies. Underlying reason is that, as focus and attention are limited to the resources that are the precursors of Enterprise Objectives, risk assessment effort will also be limited the information assets that will be the

subject of threat assessment. We have named the method as TEOREM (Tree based Enterprise Objectives Risk Evaluation Method and Metric) and also decided to utilize the already developed concepts in the management theory domain in the identification of Enterprise Objectives phase of our analysis. In doing so, we have decided to use the Resource Based View analysis of the company for this fundamental step of the method. Regarding the attack tree formation we have identified commercially-off-the-shelf available alternatives and the most up to date versions of these tools also integrate the Extended Attack Tree formation capability with embedded "utilitarian analysis" functionality. Finally we have outlined and defined the exact steps of TEOREM that embeds Enterprise Objectives within the Information Security threat assessment process. This takes place in the form of enterprise resources identified upon the usage of RBV analysis of the company. Identified resources are further linked with the information assets and the Enterprise Objectives and enterprise resources form the root nodes of the resultant attack tree and the related and identified information assets form the branch nodes of the same attack tree. Further analysis constitutes just the mechanical application of attack tree analysis methodologies utilizing COTS (commercial off-the-shelf) available toolsets

Although the main outcome of our design science based research was the artifact in the form of a method (utilized and verified within a real life enterprise setting) in order to observe and test the validity of our expected additional results regarding the TEOREM we have envisioned a mixed method research environment. Basically the expected outcome of the design science research based approach was an artifact in the form of an information security risk assessment method. Success of the applicability of this method within a real life enterprise setting was crucially important and was successfully undertaken. In addition to that an experiment was performed in unison with a case study research method to validate different aspects of this method. Within the case study method a multiple case approach was taken and both "interview" and "direct observation" was performed for triangulation purposes. In the experiment side a sample of individuals worked on an information

security risk assessment process within a company with and without using TEOREM and further the inferential analysis was executed about the difference between the means of these two populations with matched samples. Both the statistical significance results and the case study findings formed the basis for our conclusions.

As per the results of the statistical analysis it can be said that there is significant improvement within the usage of TEOREM from the effort/timing perspective. Also the case study results were in line with the expected positive impact on the usability by the management and also were of a more holistic nature that included the intangible enterprise assets as well as tangible ones.

Main contribution within this design science based research was the composition of an IT security risk assessment method that has been verified within a real life enterprise setting that came up with results more suitable for the needs of the management, as well as offering an efficiency increase in the execution.

Two design processes and four design artefacts are defined as the outcomes of design-science research in IS (March and Smith 1995). Two processes are "build and evaluate" and the potential artefacts are "constructs, models, methods and instantiations". So within this work a method (as an artefact) has been build and evaluated utilizing and synthesizing the kernel theories from information security and management domains in an interdisciplinary manner. In doing so the existing knowledge base on information security risk assessment has been extended and the outcome may form the basis for additional academic work on refining the outlined risk evaluation method and also may be utilized within business and industry environments by the information security professionals and the managerial community.

In doing this research, we have faced with the limitation of security and privacy from the enterprise viewpoint. Namely the institutions that we have approached for

the case study and experiment raised their concerns for security and privacy, as the execution of these studies would require full access to the inner workings of their networks, infrastructure and backbone. So we were able to execute the case study and experiment at one company. Ideally these studies can be replicated within different environments with different needs and expectations from the risk assessment domain. It is evident that a public institution would have different priorities than a private entity and even between public institutions the expectations will differ between universities, hospitals, public safety departments.

Also the difference in the scale of institutes will put forward an additional dimension of complexity for the applicability of TEOREM and this may also be one of the research topics in the days to come. Usability and adequacy of TEOREM for a large institute may differ from a small-to medium scale enterprise. Also the intended outcome and the expectations from an information security risk assessment will be radically different in these two cases.

Another limitation and also a candidate for future research is the long term application of TEOREM within an enterprise. In the current form of the thesis a single run of the method has been investigated within a case study and quantitative experiment. However in the longer run and in a context within which TEOREM is utilized iteratively (taking into account the effects of the learning curve) in the same organization the results may differ.

Last point of concern will be a potential decline in the accuracy of the method from a security assessment perspective versus the gain in the efficiency. As the pruning of the attack tree increases the efficiency of the method from an effort perspective, this may at the same time potentially cripple the effectiveness of the method as a security risk assessment tool.

So in order to address the last two of these limitations (namely the efficiency versus effectiveness issue and longer term usage of TEOREM) and to follow up

with the research idea entailed within this limitation, we have initiated a long term usage of TEOREM within a medium scale IT company. As the findings of this real life study come to fruition we will compile the results, analyse the findings and share these within the research community.

Also the application for a US patent has been performed and patent is pending for the method. So in a while TEOREM may be utilized within a risk modelling software tool as an additional module and then there will be a vast amount of data that will form the basis for further research focusing on the other limitations outlined above.

REFERENCES

Aime, M.D., Atzeni, A. & Pomi, P. (2008). The risks with security metrics. *QoP '08 Proceedings*, pp.65-69.

Ahmed, M.S., Shaer, E.A & Khan, L. (2008). A novel quantitative approach for measuring network security. *27th IEEE Conference on Computer Communications.*

Amenaza Technologies Ltd.. (2007). *Attack Tree Analysis of Hostile and Random Risks.*

Amit, R., Schoemaker. P. (1993). Strategic assets and organizational rent. *Strategic Management Journal*, *Vol.14*, pp.33-46.

Ammann, P., Wijesekera, D. & Kaushik, S. (2002). Scalable graph based network vulnerability analysis. *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp.217-224.

Amoroso, E. (1994). *Fundamentals of Computer Security*, Upper Saddle River: Prentice Hall.

Arora, A., Hall, D., Pinto, C.A., Ramsey, D. & Telang, R. (2004 November/December). Measuring the risk based value of IT security solutions. *IEEE IT Pro*, pp.35-42.

Bagheri, E. & Ghorbani, A.A. (2007). Risk analysis in critical infrastructure systems based on the Astrolabe methodology. *Fifth Annual Conference on Communication Networks and Services Research, Proceedings.*

Baker, W.H., Rees, L.P. & Tippett, P.S. (2007). Necessary measures. *Communications of the ACM, Vol.50, No.10,* pp.101-106.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, Vol.17,* pp.99-120.

Basili, V.R. & Weiss, D.M. (1984). A Methodology for Collecting Valid Software Engineering Data. *IEEE Transactions on Software Engineering,* November, pp.728-738.

Bennett, S.P. & Kailay, M.P. (1992). An application of qualitative risk analysis to computer security for the commercial sector. *Computer Security Applications Conference,* pp.64-73.

Bodeau, J.D. (1992). A conceptual model for computer security risk analysis. *Proceedings of Computer Security Appications Conference,* pp.56-63.

Bodin, L.D., Gordon, L.A. & Loeb, M.P. (2008). Information security and risk management. *Communications of the ACM, Vol.51, No.4,* pp.64-68.

Breu, R., Oberperfler, F. & Yautsiukhin, A. (2008). Quantitative assessment of enterprise security system. *Third International Conference on Availability, Reliability and Security, Proceedings,* pp.921-928.

Brotby, W.K. (2009). *Information security management metrics.* CRC Press.

Caralli, R.A. (2004). *Critical success factor method: Establishing a foundation for enterprise security management.* Pittsburgh, Carnegie Mellon University.

Clark, K., Dawkins, J. & Hale, J. (2005). Security risk metrics: Fusing enterprise objectives and vulnerabilities. *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security,* pp.388-393.

Clark, K., Singleton, E., Tyree, S. & Hale, J. (2008). Stratagem, risk assessment through mission modeling . *QoP '08 Proceedings,* pp.51-57.

Collins, D.J. & Montgomery, C.A. (1995). Competing on resources. *Harvard Business Review, 73:4,* pp.118-128.

Cunha, A.B. (2007). Innovation and technological convergence: An assessment of critical resources of telecommunications service providers using resource based view and dynamic capabilities. *PICMET 2007 Proceedings,* pp.52-63.

Dewri, R., Poolsappasit, N., Ray, I. & Whitley, D. (2007). Optimal security hardening using multi-objective optimization on attack tree models of networks. *CCS 2007 Proceedings,* pp.204-213.

Duan, Q., Saini, V. & Paruchuri, V. (2008). Threat model using attack trees. *CCSC Mid South Conference,* pp.124-131.

Edge, K., Raines, R., Grimaila, M., Baldwin, R., Bennington, R. & Reuter, C. (2007). The use of attack and protection trees to analyze security for an online banking system. *Proceedings of the 40th Hawai International Conference on System Sciences*.

Evans, S. & Wallner, J. (2005). Risk based security engineering through the eyes of the adversary. *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security,* pp.158-165.

Fung, C., Chen, Y.L., Wang, X., Lee, J., Tarquini, R., Anderson, M. & Linger, R. (2005). Survivability analysis of distributed systems using attack tree methodology. *IEEE Military Communications Conference 2005.*

Gan, Z., Jiufei, T. & Wu, P. (2007). A novel security risk evaluation for information systems. *Frontier of Computer Science and Technology,* pp.67-73.

Garigue, R., & Stefaniu, M. (2003). Information security governance reporting. *Information Systems Security, 12:4,* pp.36-40.

Ghemawat, P. (1991). *Commitment.* New York:Free Press.

Grant, R.M. (1991). The resource based theory of competitive advantage. *California Management Review,* pp.33:1, 114-135.

Grunske, L. & Joyce, D. (2007). Quantitative risk based security prediction for component based systems with explicitly modeled attack profiles. *Journal of Systems and Software, 81,* pp.1327-1345.

Guan, B.C., Lo, C.C. Wang, P. & Hwang, J.S. (2003). Evaluation of information security related risks of an organization. *Proceedings of IEEE 37th Annual Conference on Security Technology,* pp.168-175.

Hallberg, J., Hunstad, A. & Peterson, M. (2005). A framework for system security assessment. *IEEE Workshop on Information Assurance and Security, Proceedings,* pp.224-231.

Helfat, C.E. & Peteraf, M.A. (2003). The dynamic resource based view:Capability lifecycles. *Strategic Management Journal, Vol.24,* pp.997-1010.

Herrmann, D.S. (2007). *Complete guide to security and privacy metrics.* Auerbach Publications.

Hevner, A.R. March, S.T. & Ram, S. (2004). Design science in information systems research. *MIS quarterly, Vol.28:1,* pp.75-105.

Heyman, T., Scandariato, R., Huygens, C. & Joosen, W. (2008). Using security patterns to combine security metrics. *Third International Conference on Availability Reliability and Security,* pp.1156-1163.

Hunstad, A., Hallberg, J. & Andersson, R. (2004). Measuring IT security: A method based on common criteria's security functional requirements. *Proceedings of the 2004 IEEE Workshop on Information Assurance,* pp.226-233.

Ingols, K., Lippmann, R. & Piwowarski, K. (2006). Practical attack graph generation for network defense. *Proceedings of the 22nd Annual Computer Security Applications Conference.*

ISACA Information Systems Control and Audit Association (2009). *Risk IT* [Brochure].

Jaquith, A. (2007). *Security metrics: Replacing fear, uncertainty and doubt.* Addison-Wesley.

Jarvenpaa, S. & Leidner, D. (1998). An information company in Mexico: Extending the resource-based view of the firm to a developing country context. *Information Systems Research*, pp.342-361.

Khand, P.A. (2009). System level security modeling using attack trees. *2nd International Conference on Computer, Control and Communication,* pp.1-6

Magnusson, C., & Yngstrom, L. (2004). Method for insuring IT risks. *Proceedings of the 37th Hawaii International Conference on System Science*, pp.1-8.

March, S.T., & Smith, G. (1995). Design and natural science research on information technology. *Decision Support Systems, Vol.15:4*, pp.251-266.

Mahoney, J.T. & Pandian, J.R. (1991). The resource based view within the conversation of strategic management. *Strategic Management Journal, Vol.13*, pp.363-380.

Mauw, S. & Oostdijk, M. (2005). Foundations of attack trees. *ICISC 2005 Information Security and Cryptology 8th International Conference*, pp.186-198.

McCumber, J. (2004). *Assessing and managing security risk in IT systems: A structured methodology.* Auerbach Publications.

Meirelles, D.S., Basso, L.F. & Pace, E.S. (2008). The contributions of specific resources from the firm in its competitive performance: A resource based view approach in the software sector. *Journal of Academy of Business and Economics, Vol:8, Issue:2*, pp.86-99.

Moore, A.P., Ellison, R.J. & Linger, R.C. (2001). *Attack modelling for information security and survivability (CMU/SEI-2001-TN-001).* Pittsburgh, Software Engineering Institute, Carnegie Mellon University.

Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly, 21:2*, pp.241-242.

Naqvi, S. & Riguidel, M. (2006). Quantifiable security metrics for large scale heterogeneous systems. *Proceedings of the 40th Annual IEEE International*, pp.209-215.

National Institute of Standards and Technology, Carnegie Mellon University. (2007). *A complete guide to the common vulnerability scoring system version 2.0* [Brochure]. Mell,P., Scarfone,K., Romanosky.S. : Author.

Neubauer, T., Klemen, M. & Biffl, S. (2005). Business process based valuation of IT security. *EDSER'05,* St.Louis, USA.

Noel, S. & Jajodia, S. (2004). Correlating intrusion events and building attack scenarios through attack graph distance. *Proceedings of the 20th Annual Computer Security Applications Conference.*

Nyanchama, M. (2005 July/August). Enterprise vulnerability management and its role in information security management. *Information Security Management*, pp.29-56.

Ou, X., Boyer W.F. & McQueen, M.A. (2006). A scalable approach to attack graph generation. *CCS 2006 Proceedings*.

Ozier, W. (2002). A Framework for Automated Risk Assessment Tools. *EDPACS, Vol:30, No:4.*

Panda, P. (2009). The Octave approach to information security risk assessment. *ISACA Journal, Vol:4.*

Papadaki, K. & Polemi, N. (2007). Towards a systematic approach for improving information security risk management methods. *18th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications,* pp.1-4.

Patriciu, V.V., Priescu, I. & Nicolaescu, S. (2006). Security metrics for enterprise information systems. *Journal of Applied Quantitative Methods, Vol:1, No:2,* pp.151-159.

Peteraf, M.A. (1993). The cornerstone of competitive advantage:A resource based view. *Strategic Management Journal, Vol.14,* 179-191.

Peterson, M. (2004). *CAESAR – A proposed method for evaluating security in component based distributed information systems.* Master's Thesis, Linkopings Universitet.

Phillips, C. & Swiler, L.P. (1998). A graph based system for network vulnerability analysis. *Proceedings of the 1998 Workshop on New Security Paradigms,* pp.71-79.

Prahalad, C.K. & Hamel, G. (1990). The core competence of the corporation. *Harvard Business Review, Vol.68, No.3,* pp.79-92.

Reddy, K, Venter, H.S., Olivier, M. & Currie, I. (2008). Towards privacy taxonomy based attack tree analysis for the protection of consumer information privacy. *Sixth Annual Conference on Privacy, Security and Trust*, pp.56-64.

Roehl, W. S. & Fesenmaier, D. R. (1992). Risk perceptions and pleasure travel. *Journal of Travel Research, Vol:30, No:4,* pp. 17-26.

Rockart, J.F. (1979). Chief executives define their own data needs. *Harvard Business Review, 57:2,* pp.81-93.

Ross, J.W., Beath, C.M. & Goodhue, D.L. (1996). Develop long term competitiveness through IT assets. *Sloan Management Review, Vol:38, No:1,* pp.31-42.

Rowley, I. (1989). Managing in an uncertain world: Risk analysis and the bottom line. *IEE Colloquion on System Engineering Contribution to Increased Profitability,* 3/1-3/8.

Sahinoglu, M. (2005 May/June). Security meter: A practical decision tree model to quantify risk. *IEEE Security and Privacy*, pp.18-24.

Savola, R. (2007). Towards a security metrics taxonomy for the information and communication technology industry. *International Conference on Software Engineering Advances, Proceedings,* pp.60-66.

Saydjari, O.S. (2004 November/December). Risk based systems security engineering: Stopping attacks with intention. *IEEE Security and Privacy*, pp.59-62.

Schneier, B. (1999 December). Attack trees: Modelling security threats. *Dr.Dobb's Journal*.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world.* John Wiley & Sons.

Sheyner, O., Haines, J., Jha, S., Lippmann, R. & Wing, J.M. (2002). Automated generation and analysis of attack graphs. *Proceedings of the 2002 IEEE Symposium on Security and Privacy.*

Sultan, K., Nouaary, A. & Lhadj, A.H. (2008). Catalog of metrics for assessing security risks of software throughout the software development life cycle. *International Conference on Information Security and Assurance, Proceedings.,* pp.461-465.

Teece, D.J., Pisano, G. & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, Vol:18, No:7,* pp.509-533.

Verdon, D. & McGraw, G. (2004). Risk analysis in software design. *IEEE Security & Privacy, Vol.2, No.4,* pp.79-84.

Vu, H., Khaw, K., Chen, T.Y. & Kuo, F.C. (2008). A New Approach for Network Vulnerability Analysis. *Proceedings of the 33rd Annual IEEE Conference on Local Computer Networks,* pp.200-206.

Wagner, H.T. (2006). Managing the impact of IT on firm success: The link between the resource-based view and the IT infrastructure library. *39th Hawaii International Conference on System Sciences*, pp.1-10.

Wang, L., Noel, S. & Jajodia, S. (2006). Minimum cost network hardening using attack graphs. *Computer Communications, 29*, pp.3812-3824.

Weiss, J.D. (1991). A system security engineering process. *Proceedings of the 14th National Computer Security Conference*.

Wernerfelt, B. (1984). A resource based view of the firm. *Strategic Management Journal, Vol.5*, pp.171-180.

Wood, J. (1990). European harmonised IT security evaluation criteria. *Proceedings of the 6th International Conference on the Application of Standards on Open Systems*, pp.138-143.

Wood, T.M, King, S.G. & Kennon, J.W. (2003). A risk assessment system for multi facility organizations. *Proceedings of IEEE 37th Annual Conference on Security Technology*, pp.196-199.

Yacoub, S., Ammar, H.H. & Robinson, T. (2000). A methodology for architectural level risk assessment using dynamic metrics. 11th *International Symposium on Software Reliability Engineering, Proceedings.*, pp.210-221.

Yacoub, S.M., Cukic, B. & Ammar, H.H. (2004). Scenario based reliability analysis of component based software. *IEEE Transaction on Reliability, Vol.53, Issue.4*, pp.465-480.

Yager, R.R. (2005). OWA trees and their role in security modeling using attack trees . *Information Sciences, 176*, pp.2933-2959.

Yang, Y., Boehm, B. & Wu, D. (2006). COCOTS risk analyzer. *Proceedings of the 5th International Conference on COTS Based Software Systems*, pp.144-151.

Yin, R.K. (2009). *Case study research : Design and methods.* Sage Inc.

Yngstrm, L. (2003), *Systemic holistic approach to IT security*. DSV-SU/KTH, Stockholm, Sweden.

APPENDICES

APPENDIX A - SECURITREE ATTACK TREE MODELLING TOOL

Within this research, the Attack Tree modeling and analysis tool SecurITree by the Amenaza Technologies was an indispensable aid. SecurITree is an attack tree design, modeling and analysis tool, that also have built-in functions for pruning and attacker profiling. Appendix A includes additional information about the SecurITree tool by the Amenaza Technologies.

In the initial stages of the research, we have approached Amenaza Technologies and upon a series of correspondences we were granted a trial license to be utilized through the thesis study. Tool was also instrumental during the Case Study and within the execution of the quantitative experiment. Sample groups had a basic training on the SecurITree tool, upon which they utilized it through the case study and the experiment.

Our discussions with the Amenaza team also gave the inspiration to apply for a US patent on TEOREM, which may be an essential part of an attack tree modeling platform in the form of an additional module, or optional functionality in the days to come.

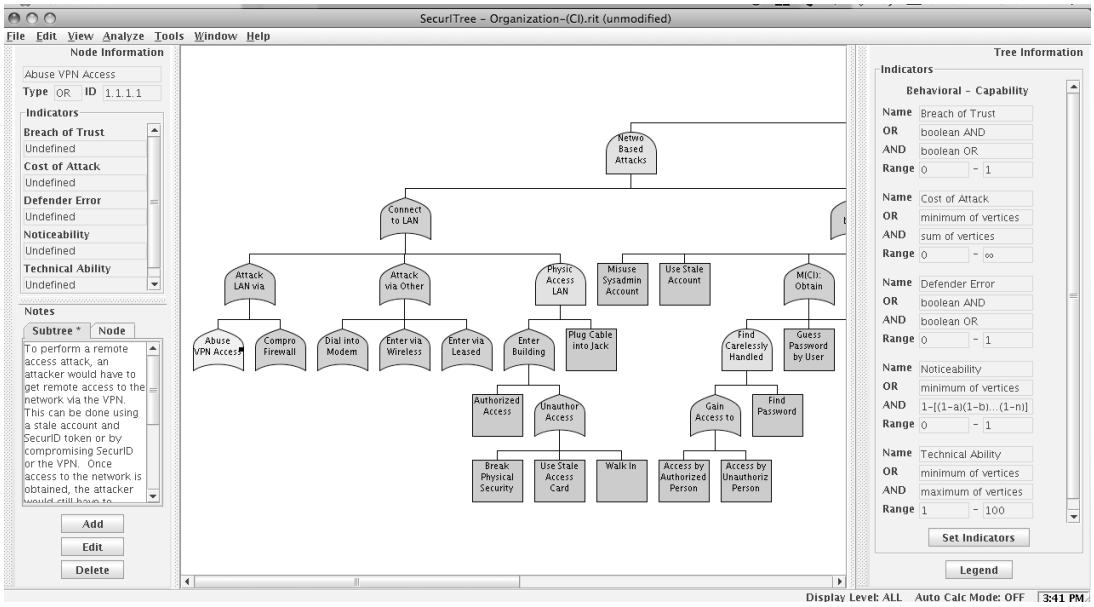


Figure 23 SecurITree Attack Tree modeling tool by the Amenaza Technologies

APPENDIX B - PATENT APPLICATION TO US PATENT AND TRADEMARK OFFICE

Patent application title: METHOD AND TOOL FOR INFORMATION SECURITY ASSESSMENT THAT INTEGRATES ENTERPRISE OBJECTIVES WITH VULNERABILITIES

Inventors: Bugra Karabey (Ankara, TR) Nazife Baykal (Ankara, TR)

IPC8 Class: AG06F2100FI

USPC Class: 715764

Class name: On-screen workspace or object

Publication date: 12/30/2010

Patent application number: 20100333002

Abstract:

In one aspect, a method to assess information security vulnerability of an enterprise includes storing enterprise objectives in a computer system, storing enterprise resources determined using a value criterion, a rareness criterion, an inimitability criterion and a non-substitutability criterion in the computer system and storing enterprise information assets in the computer system. The method also includes mapping the enterprise objectives with the enterprise resources and mapping the enterprise information assets with the enterprise resources. The method further includes determining a threat analysis using an attack tree using the enterprise resources and the information assets and determining a risk value using the attack tree.

Description:

BACKGROUND

[0001]As it is impossible to eliminate all the risks, organizations may hope that a perceived risk can be reduced if risk advice can be obtained through a risk assessment. Therefore, risk management plays a critical role in protecting an organization's information assets. Risk management is a process that covers both an assessment phase and a mitigation phase. In the assessment phase adequate methods and tools are required to determine quantitative results. In the traditional approaches the probability of occurrence of a risk is multiplied by its perceived impact to form a loss expectancy figure.

[0002]In the domain of information systems and information security management the risk assessment phase is more complicated. As information security threats are constantly evolving, use of historical or statistical figures to estimate the probability of occurrence of a specific risk may present in faulty conclusions. Currently, data repositories like the National Vulnerability Database by National Institute of Standards and Technology (NIST) are used. In some examples, available automated tools are used to determine vulnerability assessments. Most of the time, these measures tend to be geared toward security professionals and usually are not suitable for managerial decision making, which are commonly driven by compliance requirements rather than the risk management thought processes. Suitable outcomes are expected from such tools and methods to help management make decisions, prioritize resources and develop mitigation strategies against the occurrence of such risks related with the information assets of a company, however most of the time that is not the case.

[0003]U.S. National Security Agency (NSA)'s Mission Oriented Risk and Design Analysis (MORDA) provides a framework for analyzing complex information security risk postures. MORDA combines threat, attack and mission impact concepts to derive an unbiased risk metric, so the enterprise objectives in the form of missions are embedded within this framework. Identification of enterprise

objectives has not been defined explicitly within MORDA.

[0004]Another critical aspect of information security threats is their ever changing nature that evolves at a tremendous pace. In addition to that the interconnected nature of information assets presents an additional dimension of complexity in the form of a requirement for cascaded and parallel analysis of threats against the information assets.

[0005]The attack tree approach is suitable to address such architectural complexities in a dynamic manner. Attacks are modeled through the use of a graphical, mathematical, decision tree structure called an attack tree. Similar studies exist that utilize attack graphs instead of attack trees. A known issue with attack trees (and graphs) is that for systems that include numerous information resource elements the task becomes cumbersome and the scalability of the approach becomes limited within large enterprises.

SUMMARY

[0006]In one aspect, a method to assess information security vulnerability of an enterprise includes storing enterprise objectives in a computer system, storing enterprise resources determined using a value criterion, a rareness criterion, an inimitability criterion and a non-substitutability criterion in the computer system and storing enterprise information assets in the computer system. The method also includes mapping the enterprise objectives with the enterprise resources and mapping the enterprise information assets with the enterprise resources. The method further includes determining a threat analysis using an attack tree using the enterprise resources and the information assets and determining a risk value using the attack tree.

[0007]In another aspect, an article includes a machine-readable storage medium that stores executable instructions to assess information security vulnerability of an

enterprise. The instructions causes a machine to store enterprise objectives in a computer system, store enterprise resources determined using a value criterion, a rareness criterion, an inimitability criterion and a non-substitutability criterion in the computer system and store enterprise information assets in the computer system. The instructions also cause machine to map the enterprise objectives with the enterprise resources and map the enterprise information assets with the enterprise resources. The instructions further cause a machine to determine a threat analysis using an attack tree by using the enterprise resources and the information assets and determine a risk value using the attack tree.

[0008]In a further aspect, an apparatus to assess information security vulnerability of an enterprise includes circuitry to store enterprise objectives in a computer system, store enterprise resources determined using a value criterion, a rareness criterion, an inimitability criterion and a non-substitutability criterion in the computer system, store enterprise information assets in the computer system, map the enterprise objectives with the enterprise resources, map the enterprise information assets with the enterprise resources, determine a threat analysis using an attack tree using the enterprise resources and the information assets and determine a risk value using the attack tree.

Claims:

1. A method to assess information security vulnerability of an enterprise comprising:

- storing enterprise objectives in a computer system;
- storing enterprise resources determined using a value criterion, a rareness criterion, an inimitability criterion and a non-substitutability criterion in the computer system;
- storing enterprise information assets in the computer system;
- mapping the enterprise objectives with the enterprise resources;

- mapping the enterprise information assets with the enterprise resources;
- determining a threat analysis using an attack tree using the enterprise resources and the information assets;
- and determining a risk value using the attack tree.

2. The method of claim 1, further comprising identifying the enterprise objectives using mission statements.

3. The method of claim 1, further comprising identifying the enterprise objectives using enterprise goals.

4. The method of claim 1, further comprising storing enterprise resources determined using criteria added to the computer system by a user through a graphical user interface.

5. The method of claim 1 wherein storing enterprise resources comprises storing enterprise resources provided by a user through a graphical user interface.

6. The method of claim 1 wherein storing enterprise information assets in the computer system comprises storing a data file comprising the information assets.

7. The method of claim 1 wherein storing enterprise information assets in the computer system comprises storing enterprise information assets provided by a user through a graphical user interface.

8. The method of claim 1 wherein the mapping of enterprise objectives with enterprise resources comprises mapping the enterprise objectives with enterprise resources provided by a user through a graphical user interface.

9. The method of claim 1 wherein the mapping enterprise resources with enterprise information assets comprises mapping of enterprise resources with enterprise

information assets provided by a user using a graphical user interface.

10. The method of claim 1, wherein determining a threat analysis using an attack tree comprises forming the attack tree using a data file that embeds an attack tree model,

11. The method of claim 1 wherein determining a threat analysis using an attack tree comprises using additional values and attributes for leaf node values of the attack tree that are defined and added by a user through a graphical user interface.

12. An article comprising a machine-readable medium that stores executable instructions to assess information security vulnerability of an enterprise, the instructions causing a machine to:

- store enterprise objectives in a computer system;
- store enterprise resources determined using a value criterion, a rareness criterion, an inimitability criterion and a non-substitutability criterion in the computer system;
- store enterprise information assets in the computer system;
- map the enterprise objectives with the enterprise resources;
- map the enterprise information assets with the enterprise resources;
- determine a threat analysis using an attack tree using the enterprise resources and the information assets;
- and determine a risk value using the attack tree.

13. The article of claim 12, further comprising instructions causing a machine to identify the enterprise objectives using enterprise goals.

14. The article of claim 12 wherein the identification of enterprise resources can be

implemented using additional criteria added to the computer system by a user.

15. The article of claim 12 wherein the identification of enterprise resources can be implemented using a graphical user interface.

16. The article of claim 12 wherein storing enterprise information assets in the computer system comprises storing a data file comprising the information assets.

17. An apparatus to assess information security vulnerability of an enterprise, comprising circuitry to:

- store enterprise objectives in a computer system;
- store enterprise resources determined using a value criterion, a rareness criterion, an inimitability criterion and a non-substitutability criterion in the computer system;
- store enterprise information assets in the computer system;
- map the enterprise objectives with the enterprise resources;
- map the enterprise information assets with the enterprise resources;
- determine a threat analysis using an attack tree using the enterprise resources and the information assets;
- and determine a risk value using the attack tree.

18. The apparatus of claim 17 wherein the circuitry comprises at least one of a processor, a memory, programmable logic or logic gates.

19. The apparatus of claim 17 wherein the circuitry to map enterprise resources with enterprise information assets comprises circuitry to map enterprise resources with enterprise information assets provided by a user using a graphical user interface.

20. The apparatus of claim 17, wherein the circuitry to determine a threat analysis using an attack tree comprises circuitry to form the attack tree using a data file that embeds an attack tree model,

DESCRIPTION OF THE DRAWINGS

[0009]FIG. 1 is a flowchart of an example of a process to assess information security vulnerability.

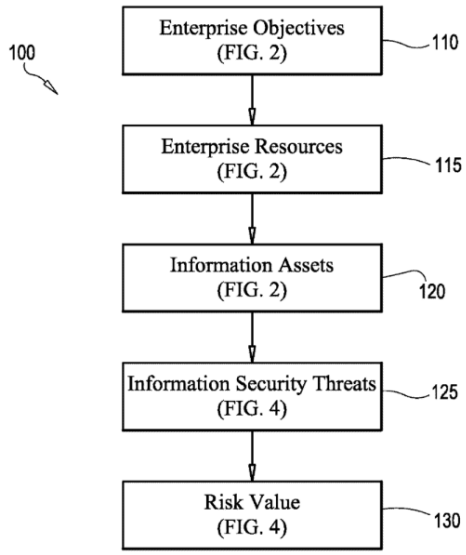


FIG. 1

[0010]FIG. 2 is a flowchart of an example of a process to determine and map enterprise objectives, resources and information assets.

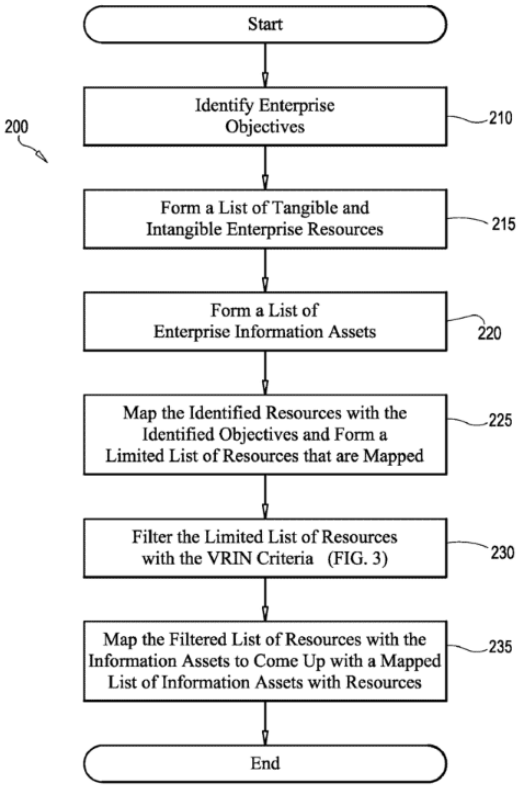


FIG. 2

[0011]FIG. 3 is a flowchart of an example of a process to perform a value, rareness, inimitability and non-substitutability (VRIN) criteria filtering of the enterprise assets.

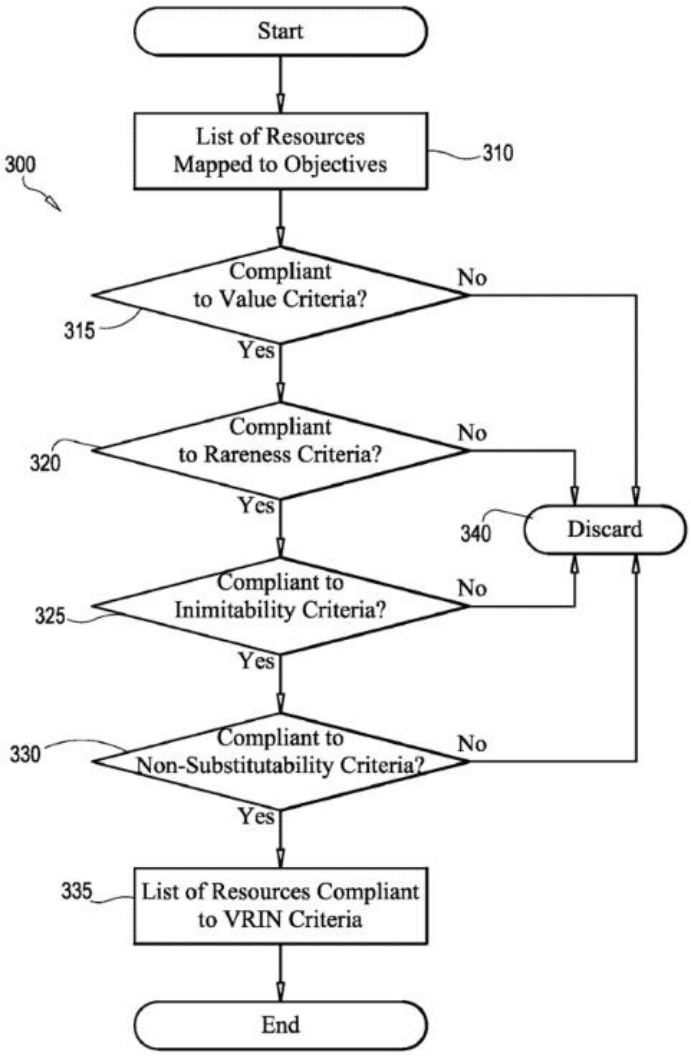


FIG. 3

[0012]FIG. 4 is a flowchart of an example of a process to determine a risk value.

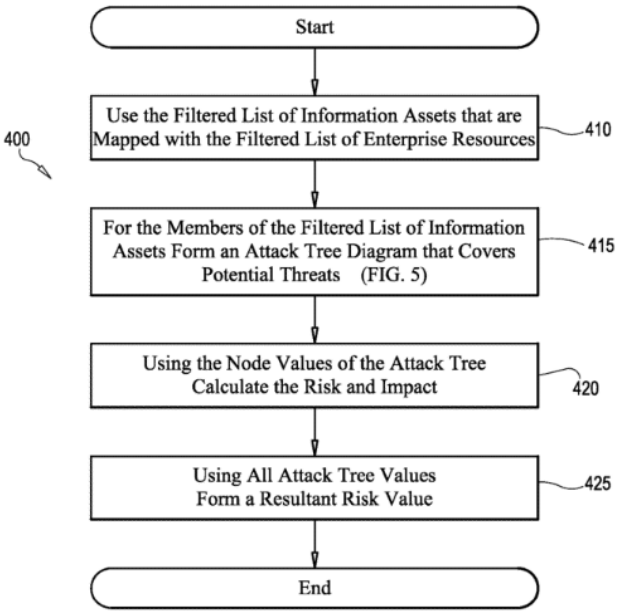


FIG. 4

[0013]FIG. 5 is a flowchart of an example of process to form an attack tree.

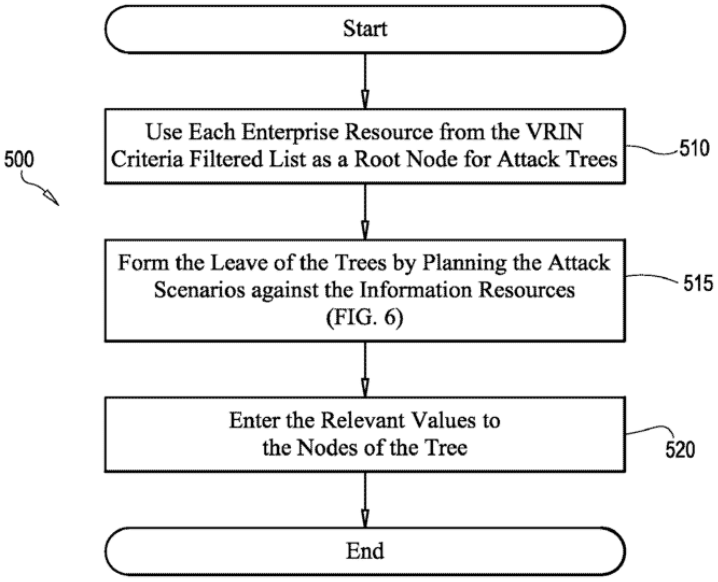


FIG. 5

[0014]FIG. 6 is a flowchart of an example of a process to form AND/OR nodes within the attack tree.

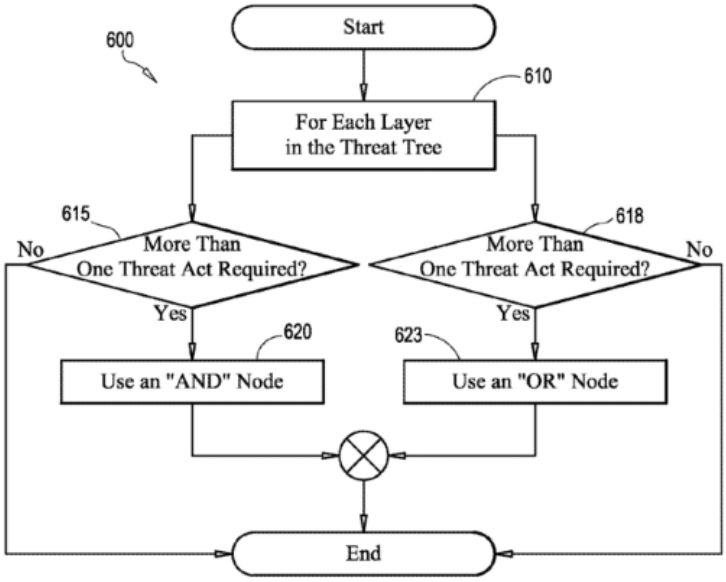


FIG. 6

[0015]FIG. 7 is a block diagram of an example of a computer on which one or more of the processes of FIGS. 2 to 6 may be implemented.

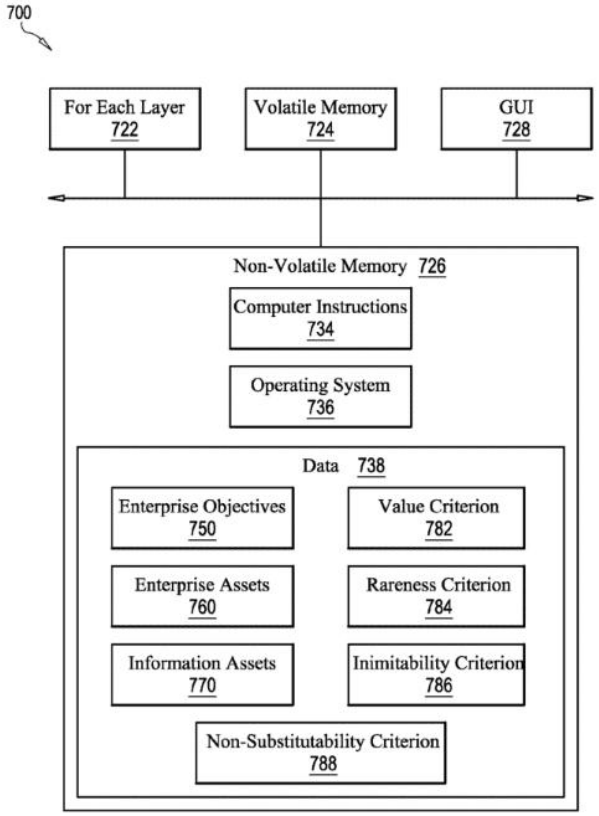


FIG. 7

DETAILED DESCRIPTION

[0016]Security is one of the key concerns in the domain of information technology (IT) systems. Maintaining the confidentiality, integrity and availability of IT systems, mandates a rigorous prior analysis of the security risks that confront the IT systems. In order to analyze, mitigate and recover from the security risks, a metrics-based approach is essential in prioritizing the response strategies to the security risks and is used for resource allocation schedules to mitigate the security risks. As will be described herein, enterprise objectives are focally integrated in the definition, impact calculation and prioritization phases of the analysis to determine metrics that are useful both for the technical and managerial communities within an enterprise. The inclusion of enterprise objectives in the identification of information assets acts as a preliminary filter to overcome the real-life scalability

issues inherent with such threat modeling efforts. An attack-tree-based approach can be utilized to offer an information security tool and method that integrates the enterprise objectives with the information asset vulnerabilities within an enterprise.

[0017]Existing tools and methods in the field of information security risk assessment suffer from certain issues. Due to the limited availability of statistics in the area of IT security, probabilistic calculations and methodologies that rely upon historical data may not be reliable. Also, due to the evolving nature of IT security threats and vulnerabilities, there may be asymmetric or non-linear leaps in the threat domain, compared to the traditional defense systems, so that the threats are dynamic in nature, which necessitates a dynamic modeling step within the methodology. In addition when the impact account is accounted for, it is evident that intangible components of the assets are at risk also. Thus, taking into account the technical level or pure monetary losses will not cover all situations. Therefore, business goals and priorities are accounted for as described herein leading to a solution having a scalability (and usability) within real life enterprise settings and scenarios.

[0018]As described herein, a methodology, which utilizes Resource Based View (RBV) model of enterprises in the fundamental phases of the method, is used to identify the resources essential for an enterprise's success in line with objectives. The methodology further maps these resources and thus the enterprise objectives with the information assets domain. The resources and related assets are analyzed from the information security threats perspective. The resource-based view of an enterprise identifies enterprises as collections of tangible and intangible resources combined with capabilities to utilize these assets to finally develop competencies that result in competitive advantage. Until now it has not been used within the context of information security risk tools and methodologies.

[0019]System security risks are of a complicated nature which can only be evaluated by considering a complex combination of possible consequences. Attack

trees are well suited and frequently used for this pursuit, so that attack tree modeling are utilized in the information asset and threat modeling stage as described herein. A purpose of the attack tree is to define and analyze possible attacks on a system in a structured way that is modeled within a tree structure including a nodal hierarchy that allows the decomposition and analysis of an attack within a number of attack steps.

[0020]Thus, the inclusion of the enterprise objectives enables results to be determined that will be inherently relevant to the decision making and execution steps of management. Identified resources through the resource based view constitute the root nodes of the attack tree and the related information assets and the steps of the threat scenario against these form the leaves of the attack tree. In addition, the techniques described herein will overcome the scalability issues with using the attack trees at the modeling and attack generation phases by prioritizing and focusing on the most critical information assets by the identification of these assets through a methodology that embeds and puts the enterprise objectives at the forefront of the system modeling and information asset definition phases.

[0021]Therefore, the usage of the resource-based view enables integration of enterprise objectives with vulnerabilities presents useful results for the management and resolves the scalability issues inherent with the attack tree modeling of information security threats.

[0022]Referring to FIG. 1, a process 100 is an example of a process to assess information security vulnerability. As used herein an enterprise is any organization such as a business, a military unit, a club and so forth utilizing information assets (e.g., information technology (IT)). Enterprise objectives are either defined within mission statements and/or goals of an organization or can be compiled through discussions with the top level management of the company (110). Enterprise resources are identified, for example, through a rigorous resource-based modeling of the enterprise (115) (e.g., as described in FIGS. 2 to 4). Enterprise resources are

based upon the relevant information assets that are identified (120) (e.g., as described in FIGS. 2 to 4). After the identification of the enterprise objectives, the enterprise resources, the information assets and a mapping of these elements to each other, a refined list and model is achieved that can be focused to determine information security (i.e., a threat analysis) (125). In one example, by using an attack tree methodology, a resultant quantitative risk figure (i.e., a resultant risk value) is determined (130).

[0023]Referring to FIG. 2, a process 200 is an example of a process to determine and map enterprise objectives, resources and information assets. Enterprise objectives such as missions and goals are compiled (210). A team, for example, that includes an enterprise's top management and functional managers (e.g., sales, marketing, finance, technical, logistics and so forth) determine a list of tangible and intangible enterprise resources, which are stored into a system (e.g., a computer 700 (FIG. 7)) (215) to determine risk.

[0024]A list of enterprise information assets is defined by the information systems team in the enterprise and stored in the system (e.g., the computer 700 (FIG. 7)) (220). The identified resources are mapped with the identified objectives to form a limited list of resources that are mapped with the enterprise objectives (225). For example, the identified objectives are matched with the identified resources that are relevant for the successful achievement of the objectives. In one particular example, a list of resources that are deemed critical for the related objective is compiled for every objective.

[0025]A value, rareness, inimitability, non-substitutability (VRIN) criteria test is used to refine and filter the enterprise resources to include enterprise resources that are relevant to the proper and successful functioning of the enterprise (230). The VRIN criteria are based upon the resource-based view of the enterprise and define differentiating, competitive and advantageous resources of the enterprise.

[0026]The filtered list of enterprise resources are mapped with the relevant information assets from the identified list of assets defined in processing block 220 to form a mapped list of information assets with the critical resources (235). For example, the identified enterprise resources are matched with the identified assets that are relevant for the proper functioning of the resource. In one particular example, a list of assets that are deemed critical for the related enterprise resource is compiled for each resource.

[0027]Referring to FIG. 3, an example of a process to filter a list of resources (processing block 230) is a process 300. The list of enterprise resources mapped to the enterprise objectives (see processing block 225) are used (310).

[0028]For each enterprise resource, the enterprise resource is evaluated against a value criterion (310). The value criterion defines that an enterprise's resources are valuable if they enable the enterprise to implement strategies that improve its efficiency and effectiveness. In one particular example, the value criterion is a Boolean and/or qualitative criterion that has a PASS/FAIL or COMPLIANT/NON-COMPLIANT value. Thus, the enterprise resources that fail the value criterion are discarded 340.

[0029]The enterprise resources that pass the value criterion are further evaluated against a rareness criterion (320). The rareness criterion from the resource-based view paradigm indicates that an enterprise has a competitive advantage if the same advantage is not shared by another enterprise. In one particular example, the rareness criterion is a Boolean and/or qualitative criterion that has a PASS/FAIL or COMPLIANT/NON-COMPLIANT value. Thus, the rarity of the enterprise resource is a decisive criterion for it to be accepted. Thus, the enterprise resources that fail the rareness criterion are discarded 340.

[0030]The enterprise resources that pass the rareness criterion are further evaluated against an inimitability criterion (325). The inimitability criterion indicates that in

order to offer a sustainable advantage an enterprise resource is harder for a competing enterprise to imitate. In one particular example, the inimitability criterion is a Boolean and/or qualitative criterion that has a PASS/FAIL or COMPLIANT/NON-COMPLIANT value. For example, a low inimitability limit also lowers the mobility or increases the time for the enterprise resource to be copied. The enterprise resources that fail the inimitability criterion are discarded 340.

[0031]The enterprise resources that pass the inimitability criterion are further evaluated against a non-substitutability criterion (330). The non-substitutability criterion from the resource-based view thinking indicates that enterprise resources that are critical do not have equivalent enterprise resources (e.g., with a lower rareness criterion value or an inimitability criterion value) that can be substituted for them. For example, existence of such substitute enterprise resources voids the importance that the particular enterprise resource presents. The enterprise resources that fail the non-substitutability criterion are discarded 340 and the enterprise resources that pass the non-substitutability criterion form the filtered/refined list of enterprise resources.

[0032]In processing block 235, the enterprise resources that are refined and filtered in the VRIN analysis are mapped with the information assets defined in the processing block 220 to form a mapped list of information assets with the enterprise resources.

[0033]Referring to FIG. 4, a process 400 is an example of a process to determine a risk value. In the threat modeling, the outcome of processing block 235 is used (410). The threats and threat scenarios that include a succession of serial and/or parallel steps of hostile moves that may jeopardize a specific enterprise resource are modeled using an attack tree (415).

[0034]Referring to FIG. 5, a process 500 is an example of a process to form an

attack tree. In forming the attack tree, the enterprise resources that successfully pass processing block 230 are used as the root nodes of the attack trees (510). The attack steps against the information assets that are relevant for this resource form the lower layers form the leaves of the tree (515). For the purpose of quantitative analysis numerical values are assigned to the leaf nodes such as, for example, a probability, a cost, and/or an impact of the related attack step (520).

[0035]Referring back to FIG. 4, using the values from processing block 520 and the AND/OR logic outlined in the FIG. 6, the attack scenario steps values are determined (420). For the resultant impact, probability and risk level of an attack or series of attacks against the enterprise resources, a resultant risk value is determined (425).

[0036]Referring to FIG. 6, a process 600 is an example of a process to form AND/OR nodes within an attack tree. For each layer in the attack tree (610), it is determined if more than one threat act is required (615) and it is determined if either of the threat acts suffice (618). A logical AND step is used if more than one attacker moves in parallel (620). A logical OR is utilized if the attacker can successfully pass a certain layer within the performance of either one of the attack steps (623).

[0037]FIG. 7 is an example of a computer 700, which may be used to execute all or part of the processes 100, 200, 300, 400, 500 and 600. Computer 700 includes a processor 722, a volatile memory 724, a non-volatile memory 726 (e.g., hard disk), for example, and a graphical user interface 728 (e.g., a screen, a mouse, a keyboard, a touch screen and so forth and any combination thereof). Non-volatile memory 726 includes an operating system 736; data 738 (including enterprise objectives 750, enterprise assets 760, information assets 770, a value criterion 782, a rareness criterion 784, a inimitability criterion 786 and non-substitutability criterion 788); and computer instructions 734 which are executed out of volatile memory 724 to perform all or part of processes 100, 200, 300, 400, 500 and 600.

The data 738 may be added to the computer 700 using the GUI 728. In one example, the identification of enterprise resources can be implemented using additional criteria added by a user using the GUI 782.

[0038]In one example, using the computer 700, the enterprise objective definitions are defined by management and are inputted into the computer 700 using the GUI 728. Usually such enterprise objectives take the form of mid- to long-term measurable goals that set the direction for the enterprise as a whole. Examples of such enterprise objectives can be, for example, achievement of X % revenue growth within the next two quarters, obtaining Y % market share within the end of year Z, cultivation of a learning organization culture, achieving six sigma quality level in three years, leading the innovative position within the industry in research and development.

[0039]Afterwards, a team of top management and functional managers define the enterprise resources. Such resources may include all assets, capabilities, organizational processes, brands, information and knowledge base that the company owns, which, for example, may be in the form of tangible or intangible entities. Some examples for the resources may cover; brand names, in-house knowledge of technology, skilled human resources, patents, proprietary technologies, efficient procedures, specialized machinery. The resource categories are identified and stored in the computer 700.

[0040]The information system assets of the enterprise are defined by the information systems management team. Such resources may include but are not limited to; servers (database, Internet, e-business, mail, customer relationship management, enterprise resource planning etc), personal computers, thin clients, mobile computing platforms, network infrastructure (such as routers, switches, bridges, hubs), smartcard systems, RFID systems, point of sale systems, automated teller machines, information security appliances (firewalls, intrusion detection/prevention systems, antivirus tools etc.), private branch exchange

telephony systems, closed circuit TV systems, data storage infrastructure, and so forth. Thus, the information systems level architecture of the enterprise is inputted to the computer 700 using, for example, the GUI 728 through a submission of a file in an appropriate format that covers this information architecture data.

[0041]Afterwards the mapping is performed. Initially the enterprise objectives are mapped to the relevant enterprise resources. As an example if "leading the innovative position within the industry in research and development" was the enterprise objective at hand than the related enterprise resources to be mapped could be, for example, patents owned by the enterprise, proprietary technologies, skilled human resources, and specialized machinery (lab tools).

[0042]The VRIN criteria are applied to filter/refine the mapped resources. Assuming, after taking into account the special circumstances of the enterprise, the enterprise resources that pass the VRIN criteria are the "proprietary technologies and the specialized machinery" and the information system assets previously defined are mapped to these filtered list of resources.

[0043]In this example the information about the "proprietary technologies" reside within the knowledge database of the research and development (R&D) team or in the computers of the team members (e.g. in the form of software code). Also the "specialized machinery" resource can be a special lab tool used by the R&D team with connections to the R&D intranet. So the related information system assets will be all the computers, servers and network components within the R&D intranet and with direct connections to this intranet as the compromise (e.g., in the form of a security breach or an availability problem such as the downtime of the specialized lab tool) of these resources leads to the compromise of an enterprise resource (proprietary technology or specialized machinery) which directly affects an enterprise objective (leading the innovative position within the industry in research and development). In one example, these steps are repeated for every enterprise objective that has been defined.

[0044]An attack tree is formed that takes the filtered enterprise resources as the root nodes and the attack scenario steps related with the relevant information assets as the leaves. Different attributes (like probability, cost, required time and so forth) can be assigned to these other nodes. Those of ordinary skill in the art can also use commercial off-the-shelf available attack tree formation programs. In one example, the formation of the attack tree can be performed with input from a data file that embeds an attack tree model. In another example, additional values and attributes can be defined and added by the user for the leaf node values of the attack tree. Analysis of the aforementioned attack tree is a straightforward implementation of the existing methods of attack tree analysis literature.

[0045]By using the successive mapping steps and using the resource filtering of resource based view criteria, an essential list of resources and related information assets are identified. Thus, using this limited (but relevant) list of assets/resources to form the attack trees, the scalability issue of the attack tree analysis is overcome. Also the list of resources/assets pertain resources/assets that are relevant to the fulfillment of enterprise objectives and the results of the analysis is therefore beneficial not only in the technical domain but also for managerial decision making.

[0046]The processes described herein (e.g., processes 100, 200, 300, 400, 500 and 600) are not limited to use with the hardware and software of FIG. 7, they may find applicability in any computing or processing environment and with any type of machine or set of machines that is capable of running a computer program. The processes may be implemented in hardware, software, or a combination of the two. The processes may be implemented in computer programs executed on programmable computers/machines that each includes a processor, a storage medium or other article of manufacture that is readable by the processor (including volatile and non-volatile memory and/or storage elements), at least one input device, and one or more output devices. Program code may be applied to data

entered using an input device to perform processes 100, 200, 300, 400, 500 and 600, for example, and to generate output information.

[0047]The processes described herein are not limited to the specific embodiments described herein. For example, the processes are not limited to the specific processing order of the process steps in FIGS. 1 to 6. Rather, any of the processing steps of FIGS. 1 to 6 may be re-ordered, combined or removed, performed in parallel or in serial, as necessary, to achieve the results set forth above.

[0048]Process steps in FIGS. 1 to 6 associated with implementing the system may be performed by one or more programmable processors executing one or more computer programs to perform the functions of the system. All or part of the system may be implemented as, special purpose logic circuitry (e.g., an FPGA (field programmable gate array) and/or an ASIC (application-specific integrated circuit)).

[0049]While the invention is shown and described in conjunction with a particular embodiment having an illustrative architecture having certain components in a given order, it is understood that other embodiments well within the scope of the invention are contemplated having more and fewer components, having different types of components, and being coupled in various arrangements. Such embodiments will be readily apparent to one of ordinary skill in the art. All documents cited herein are incorporated herein by reference. Other embodiments not specifically described herein are also within the scope of the following claims.

APPENDIX C - QUESTIONNAIRE

Please rate from 1 to 5 (Completely disagree, Disagree, Neither Agree/Disagree, Agree, Completely agree)

1) This analysis better assessed the security risk,

2) These results had a more holistic perspective,

3) These results conveyed a more complete picture,

4) This analysis came up with results better suited for my decision making processes,

5) These results included more aspects in comparison to the alternative,

6) Intangible items were included in these results compared to the alternative,

7) This analysis explained the risk issues in a more concise manner,

8) I better understood these results,

9) I prefer these results to the alternative,

10) These results articulated the security risk in a more efficient manner,

11) I was more persuaded with these findings,

12) These results were more inclusive in comparison to the alternative set.

APPENDIX D – SAMPLE (PARTIAL) ATTACK TREES

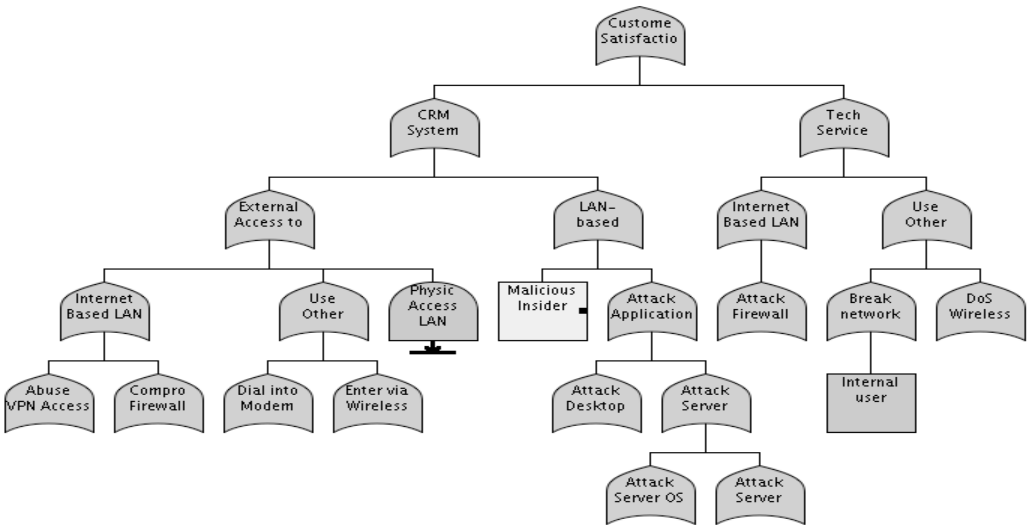
Enterprise Objectives

Retention of Customer Satisfaction, High Service Quality, Profitability

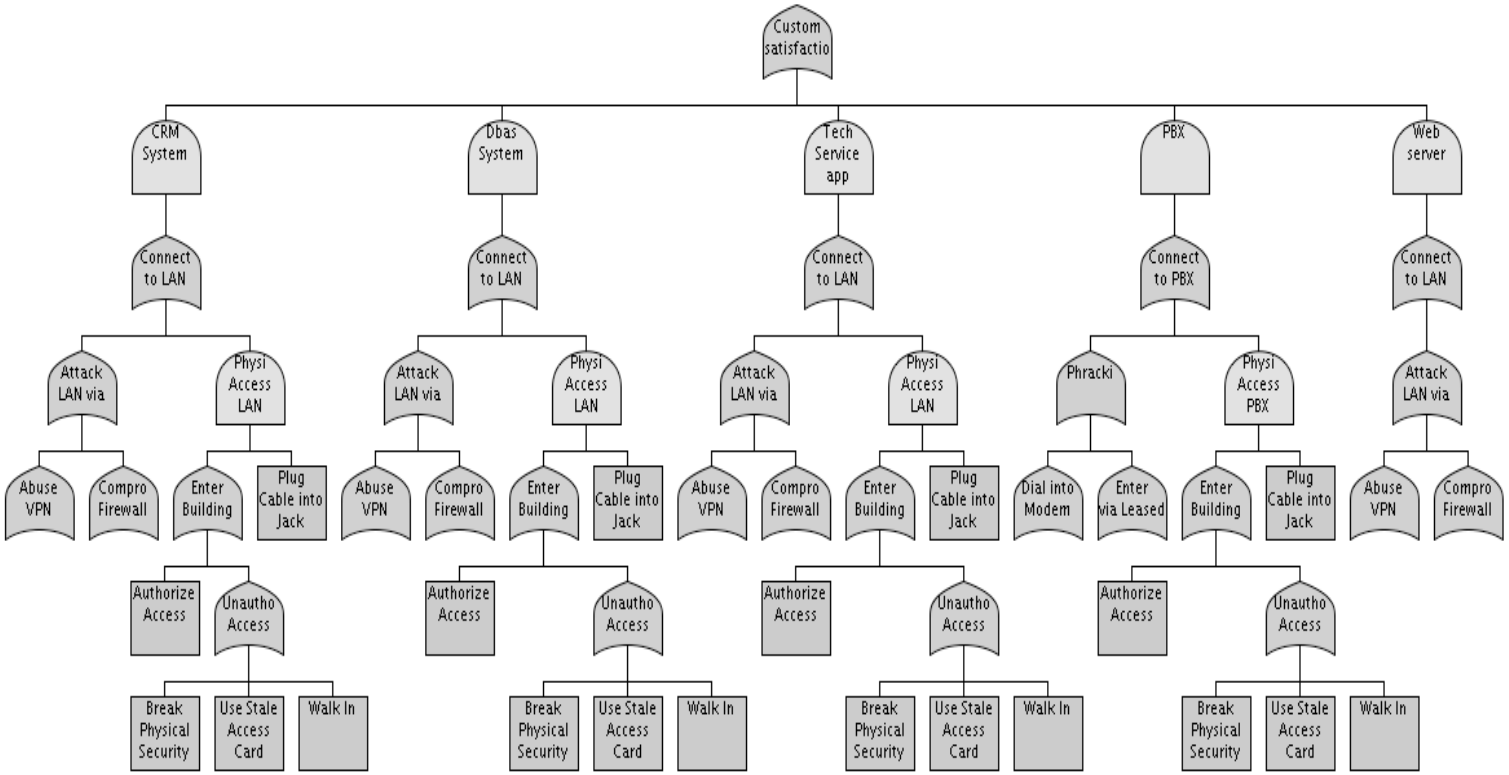
Related Enterprise assets (only for the Enterprise Objective –Retention of Customer Satisfaction)

Without TEOREM: Web server, Tech Service App, CRM, Database system

With TEOREM upon VRIN: CRM, Tech Service App



Retention of Customer Satisfaction (as Enterprise Objective) with pruning and TEOREM



Retention of Customer Satisfaction (as Enterprise Objective) without pruning and

TEOREM

VITA

Buğra Karabey has a BS degree in Electrical and Electronics Engineering from Bilkent University, an MBA degree from Baskent University, an MS degree from METU Informatics Institute. He has been active in the ICT industry for the last 18 years and acted as the Deputy General Manager and General Manager of various ICT companies in the last 10 years. Currently he is the National Technology Officer for Microsoft Turkey. His areas of research interest are Information Security Risk Assessment and Natural User Interfaces for Musical Expression.

Karabey, B. & Baykal, N. Attack tree based information security risk assessment method integrating enterprise objectives with vulnerabilities. *IAJIT Journal of Information Technology*, Vol.10:3 (accepted).

Karabey, B & Baykal, N. (2010). Method and Tool for Information Security Assesment that Integrates Enterprise Objectives with Vulnerabilities. *United States Patent and Trademark Office*, application # 12/493,799.

Karabey, B. & Baykal, N. (2009). Information security metric integrating enterprise objectives. *Proceedings of the IEEE 43rd Annual Security Technology Conference (Zurich)*, pp.144-148.

Karabey, B. (2010). Cry of Nature. *Leonardo Journal (MIT Press), Vol.43:3*.

Karabey, B. (2009). Clash of the Brainwaves. *Amber Art and Technology Conference* (Istanbul Museum of Modern Art).