Attack Tree Based Information Security Risk Assessment Method Integrating Enterprise Objectives with Vulnerabilities

Bugra Karabey and Nazife Baykal
Informatics Institute, Middle East Technical University, Turkey

Abstract: *In order to perform the analysis and mitigation efforts related with the information security risks there exists quantitative and qualitative approaches, but the most critical shortcoming of these methods is the fact that the outcome mainly addresses the needs and priorities of the technical community rather than the management. For the enterprise management, this information is essentially required as a decision making aid for the asset allocation and the prioritization of mitigation efforts. so, ideally the outcome of an information security risk method must be in synchronization with the enterprise objectives to act as a useful decision tool for the management. also, in the modelling of the threat domain, attack trees are frequently utilized. However the execution of attack tree modelling is costly from the effort and timing requirements and also, has inherent scalability issues. so, within this article our design-science research based work on an information security risk assessment method that addresses these two issues of enterprise objective inclusion and model scalability will be outlined.*

Keywords: *Enterprise information security, enterprise modelling, risk assessment, risk assessment method, resource based view, attack trees, risk management.*

Received May 4, 2011; accepted July 28, 2011; published online March 1, 2012

1. Introduction

Pervasiveness of information technology systems and resources within enterprises mandates the proper execution of techniques and policies to ensure the confidentiality, integrity and availability of these systems and the data residing within them. In order to perform the relevant protection efforts proper methods are required to analyse, plan, prioritize and execute the required steps. As risk assessment is the fundamental step within the risk management frameworks, proper design and selection of methods directly influence the success level of these efforts.

Currently there exists a plethora of information security risk evaluation methods, however most of the time these methods and their outcomes do not address the needs and expectations of the management that is in a position to decide upon mitigation plans and allocate the relevant resources. Increasing dependency of core business processes on information technology is transforming the information security management to the boardrooms of enterprises [5]. So, the proposed method that assesses the information security standing of the company must also, serve the needs of the management community. At the same time there may be intangible assets as well as tangible assets that are under the risk of information security vulnerabilities, and the proposed method must also, identify and address these within its scope.

Another critical consideration is the agility and ease of use of the threat modelling approach within the method. As the threat domain for information security systems is of an ever-changing nature and highly dynamic, the proposed risk assessment method must require an optimal level of resources to enable its periodic (re) implementation. Attack trees present a dynamic and interrelated view to the vulnerability of information assets and the impact from the attacker perspective [18]. As the modern day information systems and assets are of a highly interconnected nature, the modelling tool to be utilized must take this interrelatedness into account. There may be vulnerabilities that are only evident upon the execution of successive steps or that take advantage of the serial and parallel alternative avenues of attack. With attack trees the time and effort requirements are on the higher end of the spectrum and there are major scalability issues resultant from the application of attack graphs and attack trees on real life information systems. However with our method it is believed that these can also, be overcome by the usage of the enterprise objectives as a preliminary filter in identifying and prioritizing the information assets. Thus the required analysis effort can be diverted to them and even becomes limited to them.

So, essentially the "relevant technology and business problem" we attempt to address within this work is:

- To come up with an information security risk assessment method that generates results focusing

on the decision-making requirements of the enterprise management.
- That utilizes the attack tree modelling but at the same time provides mechanisms that act as a remedy for the excessive time and effort requirements of this risk modelling approach.

In performing the research work that forms the basis for this article, we have followed a design-science approach and applied the guidelines of design-science research [9]. In line with the above outlined relevant business problem we intended to come up with a method that will resolve the issues entailed within these problem statements and will also, 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. During this evaluation phase our information security risk assessment method was tested within a real life scenario using a mixed research approach that utilizes quantitative as well as case study research methods in parallel. 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 called Tree Based Enterprise Objective Risk Evaluation Method (TEOREM) utilizes attack trees within its execution. It also, uses the Resource Based View (RBV) of the company from the academic field of management, in defining the critical information assets relevant for the ongoing business success of the enterprise. Essentially the design-science research process for our information security risk assessment method is based upon kernel theories from the domains of information security and management, synthesized to come up with the intended qualities of efficiency/scalability and relevance.

Usage of the RBV modelling within the process inherently serves the needs and expectations of the management domain. At the same time this refinement (filtering) utilizing the resource based modelling, presents a (pre)pruning step for the attack tree formation and overcomes the scalability issue with the execution of attack tree modelling and analysis.

Intended audience for this article will be both the academicians on the field of information security and risk assessment, and also, the professionals on the management domain that are often faced with the need of relevant decision making aids on enterprise information security risk evaluation.

2. Related Works

2.1. Attack Trees

Tree based modelling structures have been previously utilized in the form of fault trees. However their recent usage has also, spread to the domain of risk analysis. 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 analyse possible threats expressed in a node hierarchy, allowing the decomposition of an abstract attack into a number of more concrete attack steps [14]. Attacks are usually modelled through the use of a graphical, mathematical, decision tree structure called an attack tree. In the domain of information systems, attack trees has been recently utilized in diverse fields as software security and even analysis of threats from malicious insiders [8, 22].

Within different studies it has been noted that the effort requirements and the scalability is a critical issue for attack trees and attack graphs [2, 10, 19, 21]. As a result of these scalability issues the usage of attack trees in real life scenarios for large enterprises becomes infeasible. Also, for the small and medium level enterprises the required level of resources (personnel and monetary) prohibit their usage. So, this scalability and effort/time overhead issue presents a major hurdle in the adoption of attack tree based information security assessment methods.

2.2. Enterprise Modelling and Enterprise Objective Integration

In order to assure the usefulness of a risk assessment method for the management level, the definite factor is the inclusion of enterprise goals and objectives within the process from the start.

Within previous studies the aim of integrating the business level perspectives to security assessment methods has been proposed [4, 6, 7, 11, 17]. Soft computing based methods and models have also, been utilized for credit risk assessment in some studies [12]. However in the identification of the enterprise goals the process is not explicitly defined in some of these studies and an integrated solution for the practitioners to execute this critical step is not clear.

Integration of enterprise objectives within the identification of critical assets (and thus information assets that are critical for these) also, ensures that the intangible assets are taken into account together with the tangible assets. When the effort is guided with the technical objectives as the main motivation, the tangible assets (like databases, servers etc.,) are identified and the intangible assets (like intellectual property, brand name etc.,) are kept out of the process.

2.3. Resource Based View of the Company

RBV approach has been used in the practice of management and also, within the academic management domain for the last 20 years and states that firms are collections of tangible and intangible assets. Combined with capabilities to utilize these assets, competencies are developed that result in competitive advantage.

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.

Some of the resources in the company consist of knowhow that can be traded, financial or physical assets, human capital and the information based processes that are firm specific and are developed over time. It has been identified that four indicators of the potential of firm resources to generate sustained competitive advantage are the value, rareness, (in)imitability and (non)substitutability, this criteria is called as the Value, Rareness, Inimitability and Nonsubstitutability (VRIN) criteria [1, 3]. 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 firms formal reporting structure, its planning system, controlling and coordinating systems.

3. TEOREM–Tree Based Enterprise Objective Risk Evaluation Method

Our risk assessment method is based upon two kernel theories from the information security and management domains, namely "attack trees" and the "resource based view modelling", in the form of a "design as synthesis" [20]. As was mentioned in the previous sections, one of the general shortcomings of previous information security risk assessment methods was the non-inclusion of the enterprise goals and objectives into the assessment processes. So within our proposed method, the enterprise goals and objectives are embedded into the initial steps of the process with the inclusion of "resource based view" modelling. Another shortcoming that was specific to the attack tree based methods was the scalability issue and this can also, possibly be overcome by the usage of the enterprise objectives as a preliminary filter using the resource based view modelling in identifying and prioritizing the IT assets that are the most critical ones. So, the required analysis effort can be diverted to them.

In addition to that when impact is taken 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. Other intangible components relevant for the business must be identified and included within the analysis. So, the proposed method approaches the domain of information security assessment with these goals in mind and attempts to address and resolve the issues outlined above.

As a basic outline the method consists of four phases; Enterprise objective and resources definition, information assets identification (mapped upon the objectives and resources defined within the previous step), attack tree formulation and finally the analysis phases.

3.1. Enterprise Objectives and Resources Definition

Utilizing the RBV of a company defined in previous sections, assessment team 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:

- 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 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 process. In such cases the management team of the organization under discussion intends to come up with a list entailing these objectives.
- 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). 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.
- This team will come up with a list of enterprise resources like physical, financial, human capital, knowledge capital (patents, processes), intangible (brand name etc.,) resources.
- One of the important challenges RBV researchers

faces is the identification of resources. 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.

- A mapping will be performed between the enterprise objectives and the resources identified within previous steps. 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.
- Resources will later be the subjects of VRIN criteria test. Proper care must be exercised at this step as most of the power of the method 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 of the outcome is based upon the proper application of VRIN criteria.
- Resultant resource pool outlines the resources that are critical for the achievement of enterprise objectives. List of resources form the input for the later stages of the method.

3.2. Information Assets Identification

Utilizing the resource pool list identified in the previous section the enterprise information assets will be selected and mapped to the enterprise resources. In doing so:

- Another team will be 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 for the team. However ongoing management commitment to the process is essential for its success.
- Team will take 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 filtered by) the VRIN criteria.
- Team will identify 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 system assets identification. In some studies, information system assets are divided into three categories, human assets (technical skills, innovation skills, business understanding, problem-solving capacity), technology assets (physical IT assets like hardware, software, networks, technical platforms, databases, architectures, standards) and relationship assets like partnerships and client relationships [16]. 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 into account within this step.

3.3. Attack Tree Formulation

After the enterprise objective definition, enterprise resource identification and the information asset selection phases, an attack tree will be 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). In the attack tree the enterprise objectives will form the root nodes and the related information assets the branch nodes. Essentially this is a technically oriented step within which the proper staff members that are literate in attack tree formulation, work in unison with the IT team members to come up with the resultant attack tree. A work in progress attack tree is depicted in Figure 1.

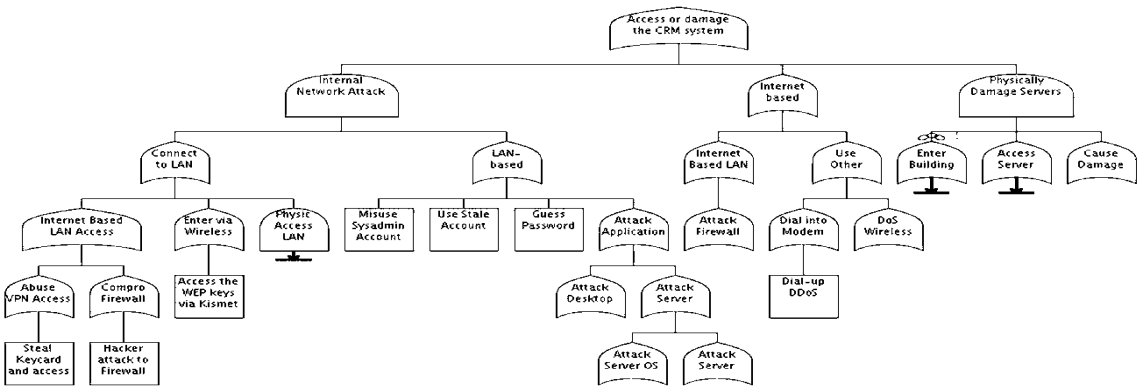

Figure 1. Work in progress attack tree.

3.4. Analysis

Majority of the effort resides in the previous modelling steps and the analysis phase is just the mechanical calculation of the values within the leaf nodes up to the root nodes. In the analysis phase, different measurements can be performed as checking the feasibility of certain attacks, the costs involved, prioritization of certain exposures. Different calculations can be performed using and traversing the resultant attack tree utilizing the different values that may reside within the nodes of the tree. Values like probability of success for the attacker against that specific node, required resources/costs regarding the fulfilment of that specific node etc., are potentially useful.

So, it can be said that within the application of the proposed method the focus moves from the macro level enterprise objectives down to the detailed analysis of individual vulnerabilities and threat identification. A higher-level look to the TEOREM is presented in Figure 2.

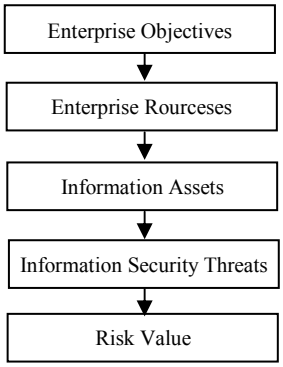

Figure 2. TEOREM stages of implementation.

4. Results and Discussion

In order to test the effectiveness of the proposed method within a real life setting utilizing scientific rigor, a mixed approach is implemented including a quantitative experiment and also, a case study research in parallel. This dual mechanism is required due to the fact that TEOREM attends to address two separate objectives:

- To address the scalability issues witnessed within attack graph and attack tree methods [2, 10, 19, 21]. So, the method and the risk assessment process become 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 is a key requirement for the relevance of the outcome [4, 6, 7, 11, 17].

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

4.1. Case Study Research

Case study research is one of the most common qualitative research approaches in the domain of information systems [15]. For the analysis of the proposed method the case study research methodology is chosen to observe and verify the effectiveness of the method in integrating the enterprise goals and objectives to the risk assessment process. A "multiple case design" within which both "interviews" and "direct observations" took place was performed to triangulate the research findings and to cross check the data achieved. A medium scale technology company was analyzed 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.

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.

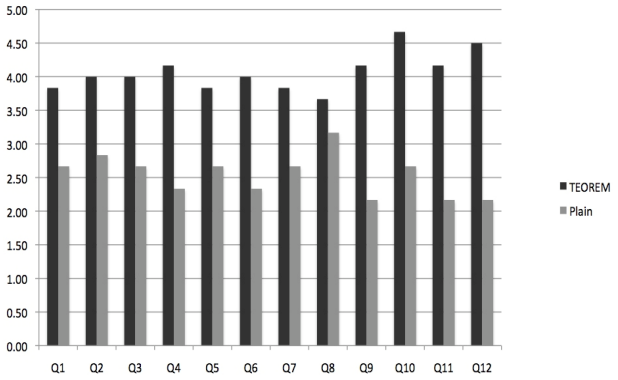

Figure 3. Case study questionnaire results for TEOREM versus plain attack trees.

Interviews were performed with board members, executive managers and department managers and a semi-structured, questionnaire based on an 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 (total of 6 board members and executive managers). Questionnaire format included questions with 5 degrees of ordinal variables as answers. 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 are 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 3 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. 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.

4.2. Quantitative Experiment

In parallel to the case study, a quantitative experiment and statistical analysis was performed, as one of the intended outcomes from the proposed method was a quantitative end result, namely resolving 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 the above outlined (in the case study research section) series of real life applications of the method were performed by a group of teams within the same operational environment. Afterwards the results that are the comparison of TEOREM enabled process timings with the straightforward application of attack trees were 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 analyzed 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 two separate test scenarios and sample bias was avoided.

In Table 1 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:

$$H_0: \mu_d = 0$$
$$H_a: \mu_d \neq 0$$

and for our experiments $t_{.005} = 4.032$ where $d = \Sigma d_i/n$ and $t=(d- \mu_d)/(s_d /\sqrt{n})$. Taking into account the data compiled within the experiments, H_0 was rejected as:

$$s_d = 0.816 \text{ and } t = 7.0 > 4.032.$$

Table 1. 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

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

5. Conclusions

Within this article an information security risk assessment method that has been developed by the authors utilizing a design-science research approach has been outlined. Further to that the effectiveness of the method and its expected positive outcomes are evaluated within a real life setting. Both via a quantitative experiment and in parallel via case study research method.

TEOREM method utilizes tools from the management domain in the form of RBV modelling in order to embed the enterprise goals and objectives into the asset identification processes. Method further focuses the assessment efforts to these refined/limited assets. It also, utilizes the attack tree modelling from the information security domain and these two knowledge areas form the basis of this work. So, the end results better serve the needs of the management community and at the same time the analysis effort becomes scalable in comparison to a direct implementation of attack tree modelling.

As per the results of the statistical analysis it can be said that there is significant improvement within the usage of the proposed method 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.

Two design processes and four design artifacts are defined as the outcomes of design-science research in IS [13]. Two processes are "build and evaluate" and the potential artifacts are "constructs, models, methods and instantiations". So, within this work a method (as an artifact) 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. Also, the method may be utilized within business and industry environments by the information security professionals and the managerial community.

References

[1] Amit R. and Schoemaker P., "Strategic Assets and Organizational Rent," *Strategic Management Journal*, vol. 14, no. 1, pp. 33-46, 1993.

[2] Ammann P., Wijesekera D., and Kaushik S., "Scalable Graph Based Network Vulnerability Analysis," *in Proceedings of the 9th ACM Conference on Computer and Communications Security*, USA, pp. 217-224, 2002.

[3] Barney J., "Firm Resources and Sustained Competitive Advantage," *Journal of Management*, vol. 17, no. 1, pp. 99-120, 1991.

[4] Basili R. and Weiss M ., "A Methodology for Collecting Valid Software Engineering Data," *IEEE Transactions on Software Engineering*, vol. 10, no. 6, pp. 728-738, 1984.

[5] Brue R., Oberperfler F., and Yautsiukhin A., "Quantitative Assessment of Enterprise Security System," *in Proceedings of the 3rd International Conference on Availability, Reliability and Security Proceedings*, Austria, pp. 921-928, 2008.

[6] Clark K., Dawkins J., and Hale J., "Security Risk Metrics: Fusing Enterprise Objectives and Vulnerabilities," *in Proceedings of IEEE Workshop on Information Assurance and Security*, New Yurok, pp. 388-393, 2005.

[7] Clark K., Singleton E., Tyree S., and Hale J., "Stratagem, Risk Assessment through Mission Modeling," *in Proceedings of ACM Conference on Computer and Communications Security*, pp. 51-57, 2008.

[8] Eom J., Park M., Park S., and Chung T., "A Framework of Defense System for Prevention of Insider's Malicious Behaviors," *in Proceedings of the 13th International Conference on Advanced Communication Technology*, Korea, pp. 982-987, 2011.

[9] Hevner A., March S., Park J., and Ram S., "Design Science in Information Systems Research," *MIS Quarterly*, vol. 28, no. 1, pp. 75-105, 2004.

[10] Ingols K., Lippmann R., and Piwowarski K., "Practical Attack Graph Generation For Network Defense," *in Proceedings of the 22nd Annual Computer Security Applications Conference*, Lexington, pp. 121-130, 2006.

[11] Karabey B. and Baykal N., "Information Security Metric Integrating Enterprise Objectives with Vulnerabilities," *in Proceedings of the 43rd IEEE International Security Technology Conference*, Turkey, pp. 144-148, 2009.

[12] Lahsasna A., Ainon R., and Wah T., "Credit Scoring Models Using Soft Computing Methods: A Survey," *The International Arab Journal of Information Technology*, vol. 7, no. 2, pp. 115-123, 2010.

[13] March S. and Smith G., "Design and Natural Science Research on Informations Technology," *Decision Support Systems,* vol. 15, no. 4, pp. 251-266, 1995.

[14] Mauw S. and Oostdijk M., "Foundations of Attack Trees," *in Proceedings of the 8th International Conference Information Security and Cryptology*, Berlin, vol. 3935, pp. 186-198, 2005.

[15] Myers D., "Qualitative Research in Information Systems," *MIS Quarterly*, vol. 21, no. 2, pp. 241-242, 1997.

[16] Ross W., Beath M., and Goodhue L., "Develop Long Term Competitiveness through IT Assets," *Sloan Management Review*, vol. 38, pp. 31-42, 1996.

[17] Savola R., "Towards A Security Metrics Taxonomy for the Information and Communication Technology Industry," *in Proceedings of International Conference on Software Engineering Advances Proceedings,* Finland, pp. 60-66, 2007.

[18] Schneier B., "Attack Trees: Modeling Security Threats," *Dr.Dobb's Journal*, vol. 24, no. 12, pp. 21-29. 1999.

[19] Vu H., Khaw K., Chen Y., and Kuo C., "A New Approach for Network Vulnerability Analysis," *in Proceedings of the 33rd Annual IEEE Conference on Local Computer Networks,* Australia, pp. 200-206, 2008.

[20] Walls J., Widmeyer G., and ElSawy O., "Building an Information System Design Theory for Vigilant EIS," *Information Systems Research*, vol. 3, no. 1, pp. 36-59, 1992.

[21] Wang L., Noel S., and Jajodia S., "Minimum Cost Network Hardening Using Attack Graphs," *Computer Communications*, vol. 29, no. 18, pp.

[22] Zhang Y., Jiang S., Cui Y., and Zhang B., "A Qualitative and Quantitative Risk Assessment Method in Software Security," *in Proceedings of the 3rd International Conference on Advanced*

Computer Theory, vol. 1, pp. 534-539, 2010. 3812-3824, 2006.

Bugra Karabey received his Bs in electrical and electronics engineering from Bilkent University, and MS on information systems from Middle East Technical University. Currently, he is a PhD candidate in the Informatics Institute of Middle East Technical University. His research interests include information security assessment and risk metrics.

Nazife Baykal received her Bs in mathematics, MS and PhD on computer engineering from Middle East Technical University. Currently, she is the Director of the Informatics Institute, of METU. Her research interests include medical information, bioinformatics, computer networks and security, neural networks, data mining knowledge discovery, she has numerous publications.