THESIS FOR DEGREE OF LICENTIATE OF ENGINEERING

CHALMERS

Security and Risk Assessment:

Black box modeling, Taxonomy and Systematic Literature Review

Laleh Pirzadeh

Division of Computer Engineering
Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Göteborg, Sweden 2016

Security and Risk Assessment: Black box Modeling, Taxonomy and Systematic Literature Review

Laleh Pirzadeh

Technical Report 159L
ISSN 1652-876X
Department of Computer Science and Engineering
Computer engineering division
Chalmers University of Technology
SE-412 96 Gothenburg
Sweden
Telephone: +46 (0)31-772 1000

Printed at Chalmers Reproservice
Gothenburg, Sweden, 2016

Security and Risk Assessment: Black box Modeling, Taxonomy and Systematic Literature Review

LALEH PIRZADEH
Department of Computer Science and Engineering
Chalmers University of Technology

ABSTRACT

In order to successfully perform and manage any type of project, there is a need to identify and assess the key factors that have an effect on the project's performance and its deliverables. Security and risk are two important concepts in contemporary information system industry that need to be assessed and addressed. Unfortunately, there exists no clear overall view of the key factors that are involved in the security and risk assessment processes.

This thesis attempts to highlight the effect of system attributes and operation on security and risk assessment. Moreover, due to criticality of risk assessment in both information system and software development projects, the thesis attempts to clarify the assessment process by identifying and categorizing existing approaches and investigating their difference. To that end, the thesis proposes a structured approach for assessment and metrication of operational security that is based on black box modeling for categorizing security metrics as being protective or behavioral, and integrity metrics as being system-related or threat-related. The thesis also proposes a novel factor for improving reliability of security risk calculation and analysis by taking system operational factors into account. Another contribution of the thesis is taxonomy for the risk assessment process in which key players and phases in the risk assessment process are identified. Finally, different risk management strategies among various software development processes are investigated to identify potential advantages of one to the other.

ACKNOWLEDGEMENTS

During my PhD journey, I had the fortune to meet amazing people without whom I would never be the person I am today. I am simply grateful to the challenges this path made me face, which led me to know the inner strength I never knew I had in me. This PhD education made me realize that there is no single answer to complicated questions, and the deeper you dig into it the harder it becomes to say that you have found the answer. Just like with any other phase in life, the results did not matter; the journey, the stories, the people and the feelings are what remain in my heart and soul. I owe this feeling to you, my supervisors, examiner, small circle of valuable friends and my family.

Erland, thanks for seeing the ability in me as a PhD student and for keeping up with my random questions when I was wandering around with my ideas. You helped me to formulate my thoughts in a structured way and to see the bigger picture when I was drowning in details.

Richard and Ana, thanks for volunteering to take over my supervision and for introducing me to another research field. I learned a lot from conducting literature review under your supervision.

Jan, you are the super hero in my story. You rescued me when I did not see any light and was stuck. When I did not believe I could do it, you still believed in me and assisted me in every single step of the way carrying all the weight until you made me strong enough to share the trouble with you. You never gave up and therefore made it hard for me to give up. I will always remember our nice meetings, fikas and deep discussions about life. Not only did you rescue me as a PhD student; you also rescued a human who struggled to find a meaning. You made me stronger, more patient and loving. I will always look up to you as my idol and you own a big piece of my heart and mind. Thank you!

Per, thank you for volunteering to take the role as my examiner and for all the positive feedback and kind comments. I was always happy when I received emails from you or had meetings with you, as you found the good in my messy texts and made me believe I can always improve myself. Your positive attitude made me reflect upon my attitude towards life. Thank you for your great support.

Julia, Boel, Antigoni, Behrooz, Fatemeh, Hamid and Negin, my wonderful caring friends! I got to know you during my studies at Chalmers but I am sure you will always be in my life. You made my life more fun and meaningful. The times we spent together talking about our funny and miserable PhD student lives, nerdy jokes, having fikas and afterworks are some highlights of my time at Chalmers. Your friendships mean a world to me and I am blessed getting to know you. Thank you!

Last, but not least, I am grateful to my family for their unconditional love, caring and support. Mamani and babayee, not only did you raise me strong enough to be able to be on my own; you also never let me feel alone, and supported me with all the love and caring that is beyond my needs every single day. You never gave up on me regardless of my progress and always supported my choices. When I forgot how to fly and my wings were broken, you stood by me, took care of my wounds and taught me how to fly high again. Your belief in me is the reason I am standing where I am today. I love you both fereshtehaye mehraboon.

Panti goli, my wise, kind and loving sister. Thank you for all your supportive actions and words. You always make sense and I sometimes hate that ;) Thanks for always being there for me and taking my hand when I needed it but was too stubborn to ask for help. Thanks for the days and nights you listened to me and took care of me. Love you khakhooli.

Zhaleh goli, my dearest, my older sister by 15 minutes, my super power woman, and my idol. You know that no matter how life plays you are always the closest to my soul, heart and mind. I could never imagine my life without you, your loving heart, your super kind eyes, your effortless generosity and your endless caring. You are the air I breathe. You are the one who keeps my heart beating and my eyes open for a new day. I owe everything in my life to you. Love you jigari.

Lily my wonderful loving caring energetic little fur ball. It is strange that I am writing to you in my acknowledgement, but if one day comes that pets can read I want you to know that your companionship means the world to me. You love me unconditionally even though I do not give you ice cream when you look at me with those begging eyes. I will love you forever.

They say you never choose your family, but if I had the chance to choose it would definitely be you guys.

LIST OF INCLUDED PAPERS

The thesis is based on the following papers.

Paper A: Erland Jonsson, Laleh Pirzadeh, "Identifying Suitable Attributes for Security and Dependabiliy Metrication", SECUREWARE 2013, the 7th International Conference on Emerging Security Information, Systems and Technologies, Barcelona, 25-31 August, 2013

Paper B: Laleh Pirzadeh, Erland Jonsson, "A Cause and Effect Approach Towards Risk Analysis", Metrisec 2011, Third International Workshop on Security Measurement and Metrication, Banf, 20-21 September, 2011

Paper C: Laleh Pirzadeh, "An Attempt to Structure Risk Assessment", Nordsec 2012, The 17th Conference on Secure IT Systems, Karlskrona, Sweden, 31 October- 2 November, 2012

Paper D: Laleh Pirzadeh, Ana Magazinus, Richard Torkar, "A Systematic Literature Review on Risk Management in Agile and Plan-driven Software Development", Technical report 2016:06, ISSN: 1652-926X

Table of Contents

1. INTRODUCTION

The growth of information systems is progressively simplifying our daily lives. At the same time these systems have become increasingly complex. In the past, the most important concern with mechanical and computer-based system was to ensure their reliability during operation. Such a concern draws more attention to specific attributes of computer and communication based systems such as dependability, reliability, functionality, and safety. These attributes define the level at which a system can handle an operation without failing with disastrous consequences. However contemporary computer-based systems are yet more complicated in the sense that they must handle the occurrence of system failure of different nature than the random failures. Accordingly, other attributes such as security, privacy and risk have become important to ensure successful business and economic decisions in industry.

For business an additional critical aspect is risk management. In order to manage risk, it is crucial to conduct preventive work for information security throughout society. Further, to be able to manage the organizations, managers need to make economic decisions on daily basis, be it spending money on specific security matters, prioritizing different tasks, or deciding on an acceptable risk level. Additionally, in order to control and manage information systems, regardless of their properties, it is of value to have knowledge about system performance in both normal and hostile environments. Information system assessment could enhance the process of gathering such information by providing an overview of system security and dependability, operating and defense mechanisms, system vulnerabilities and strength.

To get a profound understanding of information systems operation in hostile environments, there is a need to conduct operational security and risk assessment. The assessment process can be either qualitative (expert-based) or be based on quantitative metrication of security and risk. Accordingly, the assessment process results in qualitative or quantitative measures, which are beneficial for designers when choosing among different security features in order to reduce risk of system failure when system vulnerability is targeted by threats. Furthermore, information system security and risk assessment enhances managers' decisions on whether to invest money on improving security to avoid monetary consequences or to accept the risk of security breaches and system failures.

The objective of this thesis is to provide an insight into the process of security and risk assessment, when used in various settings. Identifying different system attributes becomes more complicated when the system boundaries are not clear [1]. Since this thesis addresses different aspects of information systems, it is necessary to understand the use of different terminologies when investigating different contexts. To that end, the thesis focuses on two particular system aspects. First we present a study of operational security and risk assessment in information systems in general, taking a black box approach. We then present an investigation of risk assessment and management in a more special setting, namely the software development process.

We consider these two system aspects, information system in general and software development process in particular, due to the fact that terminologies often differ completely when investigated in different contexts, which is the case with risk in relation to system

security vs. the concept of risk in different projects such as development of software. The first definition for risk refers to risk of threats attacking the system of interest and causing alteration of system behavior such as compromised confidentiality or availability. The latter definition refers to risk of project failure in terms of budget shortcomings or missing scheduled deadlines. However, sometimes the terminologies are convergent or overlapping, which is the case for security and dependability as well as for dependability and trust. For the purpose of this thesis we therefore present a clear terminology for such attributes. In the following subsection, we summarize common definition for dependability, security and risk. As this thesis addresses risk in two different contexts, we will provide a short description of risk management and assessment within information systems, on the one hand, and software development projects, on the other hand.

To summarize, the main problem this thesis strives to address is the lack of clarity and consistency regarding definitions and terminologies, as well as an overall view of key factors that are involved in the security and risk assessment process. To that end the thesis starts by proposing a categorization of a set of attributes to be applied as metrics for quantifying operational system security. Moreover, by highlighting system operation and the internal mechanisms effect on system output, we suggest a new metric for calculating risk probability. Further, we propose a taxonomy that clarifies the resources, inputs, evaluation method and outputs involved in the qualitative and quantitative risk assessment process. To provide a wider vie, we investigate how risk is assessed and managed in a bigger and more concrete setting, i.e., software development.

In the following sections the key attributes in this thesis, i.e. dependability, security and risk, are defined. A short history of the origins of the attributes is provided in Section 1.1. The context within which the attributes are applied is established in Section 1.2.

1.1 Dependability, Security and Risk ----- Definition and History

Dependability is one of the oldest operational attributes of a system. It is used to identify the service delivered or in other words the behavior of a system in normal and faulty environments. A committee on "Fundamental Concepts and Terminology" first addressed the dependability concept back in 1980 [1]. This was followed by seven position papers leading to a book on the concepts and terminology [2]. Dependability was defined as "the ability to deliver service that can be justifiably trusted" [1]. The same authors proposed an alternative definition, as "the ability of a system to avoid service failures that are more frequent and more severe than is acceptable" [1]. The concept was composed of several attributes, each shortly described below [1].

- ***Availability*** refers to system readiness for delivering correct services.
- ***Reliability*** refers to system ability to continue with providing correct service.
- ***Safety*** refers to system ability to prevent catastrophic consequences in case of system fault or failure.
- ***Integrity*** refers to system ability to prevent improper system alterations.
- ***Maintainability*** refers to system ability to undergo modifications and repairs.

The first attempts towards ***security*** were initiated in ancient times when Caesar sent encrypted letters by changing the order of alphabet letters to prevent unauthorized disclosure of military

related information to enemies. Accordingly, cryptography and confidentiality protection were the first aspects of security that caught attention and led to broad research domains.

Even though computers started being used in the 1950s, it was only much later in the 1970s that researchers started to investigate computer security [3]. Later, other system aspects were assigned to security making it a more complex attribute. The most commonly used definition for computer security (also network and IT security) was proposed by ITSEC [4] as "protection of the computer systems, services, information and the networks connecting them from intentional attacks". Accordingly, security was defined as a combined concept covering three main system attributes as described by following.

- ***Confidentiality*** refers to system ability to prevent information from disclosure to unauthorized parties.
- ***Integrity*** refers to system ability to prevent unauthorized modification of information.
- ***Availability*** refers to system ability to prevent unauthorized withholding of information or resources.

This definition is similar to the ones later proposed by Common Criteria [5] and British code of practice [6]. The definition covers the most important system attributes to withstand a hostile environment. We believe it is possible to combine security and dependability attributes to get a better understanding of system functionality in hostile and normal environments. Although the definition for availability and integrity differs between the security and dependability concepts, they have the same implication. The difference is that dependability is evaluated in the absence of malicious input whereas security is evaluated in malicious environments. Moreover, there have been studies on the relationship between security and safety in different domains, such as safety-critical systems. Laprie et al. [1], [2] attempted to merge security and dependability concepts in the early 80s, which was followed by other attempts with the same goal. In spite of these endeavors there does not exist an accepted proposal for a unified concept that encompasses security, safety and dependability.

As defined by Security Risk Management Body of Knowledge [7], "security risk is any event that could result in the compromise of organizational assets… which may adversely affect the enterprise. As such, consideration of security risk is a vital component of risk management."

In this thesis we consider ***security*** as the ***root*** for other system ***composite attributes*** such as ***risk*** and ***dependability***.

It should be noted that the security concept mentioned above considers protection of confidentiality, integrity and availability against intentional attacks. However, in order to have a more holistic view within this thesis, we introduce inputs provided by ***users*** and ***non-users***. The input provided by users and non-users can be divided into three classes that is described as follows.

- ***Malicious input***: Non-users or malicious users introduce malicious intent to make a breach to the system, which could be for various reasons such as monetary benefits.
- ***Faulty input***: Users introduce an unwanted/unintentional faulty input to the system, e.g. as a result of a mistake.

- ***Normal input***: Users introduce a normal input to the system resulting in a normal environment for the system.

As well explained by Neumann [8, p.130], there are no essential functional differences between accidental and intentional threats and they might lead to similar or the same consequences. While, the techniques for addressing them might be different, it is often crucial for systems to be protected against both kinds of threats highlighting the necessity to anticipate both types. In this thesis the malicious input is treated similarly to the faulty input. Therefore the intention of the introduced attack in this thesis context is irrelevant.

According to Oxford English Dictionary the term "***risk***" is taken from an Arabic word "رزق", the meaning of which is "working in order to gain income and profit" [9]. The English word "risk" was first used in 1655 to define "the possibility that something unpleasant or unwelcome will happen" [9]. Risk is closely connected with the term "uncertainty" which represents lack of reliability of a situation. This characteristic is assumed to be unpleasant as it makes it difficult or impossible to be prepared for the consequences. According to ISO 31000 [10] risk is "the effect of uncertainties on objectives". Therefore, risk is generally investigated to reduce the amount of uncertainty involved in various contexts.

There exist different contexts and industries where risk plays an important role in product development and organization strategies. One of the earliest areas where risk has been investigated is automotive industry. According to ISO 26262 [11], which is used in the automotive domain, risk is defined to be a product of a probability of occurrence of harm and the severity of that harm. Risk assessment in other fields is similar to this approach by focusing on identifying the ***probability of an unwanted event exposure (likelihood)*** and the ***consequences*** of such event in case of occurrence **(loss)**.

1.2 Thesis Context and Outline

This thesis contains work that investigates risk in two different contexts, namely (i) information systems and (ii) software development.

In the context of information systems, we take a conceptual and general point of view by considering information systems as a whole, leaving its components such as software, organization, people, and data aside. In this context, risk is commonly assessed by identifying potential threats towards the information system, approximating the probability of attacks launched towards the system, and valuing the potential losses due to possible system failures [23]. The risk assessment process for information system is categorized into qualitative and quantitative approaches, which will be presented in details in Section 2.

In the specific context of software development, we study the development process in more detail, making organization and people the components of interest. In this context risk constitutes a key player in project planning and initiating phase and cannot merely be modeled as a product of probability and consequences of unwanted events. The level of uncertainty is high when planning and initiating projects due to a variety of activities and roles involved in each phase of the project. We realize that risk management and assessment has been a key factor in software development industry for a long time and therefore been investigated deeper and in more details in comparison with risk assessment in information systems. This could be due to the complexity of assessing information system security risk

and lack of data. However, we believe the role of risk assessment is underestimated in information system industry in general. Similar to other types of projects, the earlier that risk is investigated and addressed the higher the chances are for a successful software development project. In the software development context, risk is coupled with initiation and planning uncertainties during requirement engineering and design phases. This is presented in more detail in Section 2.

In this thesis, we begin by investigating security and dependability assessment by applying black box modeling (meta-conceptual model) for metrication and, using the same model, propose a cause and effect approach for risk assessment. We then propose a framework for performing risk assessment, specifically focusing on quantitative approaches. Finally, we investigate the risk involved in the software development process.

The remainder of this thesis is organized as follows. Section 2 presents a general background and research history for information system security and risk assessment, quantification and management. Section 3 describes the main problems and questions this thesis addresses and summarizes each paper by providing a short list of contributions. Finally, Section 4 concludes the thesis by providing a summary of this work and identifying directions for future research.

2. MANAGEMENT AND ASSESSMENT

In a successful business an important requirement is to manage different tasks and processes within the organization. As mentioned in the introduction, it is necessary to assess and analyze different factors that are involved in the project to perform proper management. As the same reasoning applies to information system and security, well-established information security and risk assessment is required for a reliable and functional information system. For these reasons, we see value in providing a short background on the main concepts investigated in this thesis. Additionally, we find it important to acknowledge the significance of research history on security and risk management and assessment within the context of information systems and project.

The purpose of this section is to provide a description of the two contexts investigated in this thesis, namely information systems and software development. Accordingly, Section 2.1 focuses on the information systems context, and begins with a general description of information system-security management in Section 2.1.1. Then follows a description of information system-security assessment and its two different types in Section 2.1.2. The process of information system-security risk assessment is explained in more details in Section 2.1.3, where it is supported by a framework to illustrate key factors and phases of the process. The focus of Section 2.2 is the project context, starting with description of the process of project management and assessment in Section 2.2.1 and 2.2.2, respectively. This is followed by a description of the project risk management process in Section 2.2.3 and software development risk management in Section 2.2.4. Finally, we provide a summary in Section 2.3

2.1 INFORMATION SYSTEM CONTEXT

This section focuses on clarifying the research history and definitions within information system and security context. Accordingly, a brief summary of some standards and taxonomies of information system security management and assessment are presented. This is followed by a more detailed description of information system-security risk assessment process.

2.1.1 INFORMATION SYSTEM SECURITY MANAGEMENT

Today's technology-dependent industries need to analyze, evaluate and treat information as a "business issue" as opposed to as a "technical issue" in order to achieve strategic business objectives [13]. Within a technology and business context, a management process generally refers to ability to coordinate and conduct organizational activities compliant with organizations' policies and procedures to enhance the organization success [12].

Similarly, according to Control Objectives for Information and Related Technology (COBIT) [12], information-security management refers to "the necessary requirements and/or obligations to effectively initiate, plan, execute, monitor and control information security activities across the organizations in an effort to successfully achieve organizational security objectives; and to protect the organization from all potential threats" [12], [13].

COBIT [12] and ISO/IEC 17799 [14] are the two common applied frameworks that provide guidance for initiating, implementing, maintaining and improving information technology security. COBIT has proposed a process-driven framework that includes four main domains

being plan and organize; acquire and implement; deliver and support; and monitor and evaluate. Moreover, ISO/IEC 17799 proposes security control domain based framework, which includes eleven security control domains, such as access control and information security incident management.

2.1.2 Information System Security Assessment

Among the many ways to evaluate information systems and computers, one approach is to assess how secure and dependable they are. There exist diverse guidelines for performing information system security assessment. The Threat, Vulnerability, Risk Assessment (TVRA) model proposed by European Telecommunication Standards Institute (ETSI) [47], Common Criteria [5], and SANS taxonomy of information system audits and assessment [16] are examples of such guidelines.

Some early work was done in the Workshop on Security System, Scoring and Ranking (WISSR) in 2001. They defined Information Security* (***IS****) as a synonym for "security metrics". More specifically, IS* was defined as "a value selected from a partially ordered set by some assessment procedure, that represents and IS-related quality of some object of concern. It provides or is used to create a description of, prediction or comparison with some degree of confidence" [17]. WISSR suggested that IS* measurements and metrics can be organized into three tracks: technical, operational and organizational. Technical metrics are used to describe and compare technical objects such as algorithms and architectures. Operational metrics are used to describe and manage the risks towards the operational environment and the organizational metrics are used to describe and track the effectiveness of organizational programs and processes. There exist several taxonomies that propose different categories for information system security metrics such as information assurance metrics proposed by Vaughn et al. [18], the U.S. National Institute of Information Standards and Technology (NIST) security metrics taxonomies: 800-55 [19], 800-26 [20] and information assurance metrics taxonomy for IT network assessment proposed by Seddigh et al. [21]. However, it is out of the scope of this thesis to give details of taxonomies, their advantages and shortcomings. A short summary of different taxonomies and categorizations of security metrics is presented by WISSR [17].

Depending on the process of data collection and the way results are presented ***IS**** can be categorized as qualitative or quantitative metrics. There is a vague distinction between these two types and it frequently breaks down in practice. Even WISSR, which introduced the security metrication categories, avoids discussing qualitative vs. quantitative measures. Although this is a very important topic, it is beyond the scope of the thesis to investigate it in detail. However, we touch upon a general description of qualitative and quantitative metrics below, followed by our metrics definition proposal.

Qualitative assessment represents security in a qualitative way such as a high/low/medium scale for threats and vulnerabilities proposed by an expert, which is more useful in abstract and high-level system assessment. According to SANS [22] qualitative security assessment relies upon three types of individuals being a "(1) facilitator who is familiar with information security concepts (2) a manager (from the business side) who is responsible for the data and the associated business processes, (the data/process owner) and (3) solution providers who are experts familiar with delivering and supporting solutions that protect and support business processes."

Quantitative assessment offers more refined information about system security components such as a number of threats attacking the system, threat severity, difficulty of an attack, system defence strength or plausibility of a vulnerability. Quantitative assessment methods are commonly based on mathematical models and probability analysis. In comparison with qualitative methods, these methods are more technical oriented, and their target audience are therefore typically developers, system engineers and technicians. Quantitative metrics make the decision-making process easier by providing numerical values on loss and benefits of applying or skipping security controls.

One example of quantitative metrics is attacker success measure. These measures use a privilege graph to assess the following four measures for an insider seeking root privilege: SP (shortest path), NP (# of paths), Mean Effort assuming attacker has total memory and Mean Effort assuming attacker is memory-less. The goal of these metrics is to improve security monitoring and administration [17]. A list of various quantitative metrics, their goals and target audience is presented by WISSR [17].

We choose to make a clear distinction between these two types based on the following reasoning.

We say that IS* functions as a ***qualitative assessment method*** if the data for the assessment process is collected by qualitative data collection methods such as interviews or surveys, and the assessment involves high level of subjectivity such as experts' judgement.

In contrast, we say that IS* functions as a ***quantitative assessment method*** if the data is collected by statistical analysis and/or logs of real data and is used by mathematical models such as probabilistic analysis and graphs, therefore leading to an objective or semi-objective assessment.

2.1.3 Information System Risk Assessment

Risk Assessment is a process performed in order to assess the risk threatens a system by identifying potential threats towards the system. According to Jaisingh et al. [23] the assessment is done by:

- Estimating the likelihood of these threats attacking the system
- Identifying and ranking the value, sensitivity, and criticality of assets
- Estimating the potential losses
- Identifying cost-effective solutions to mitigate the risk.

As a result, risk assessment is a useful tool for prioritizing security resources in organizations [24] and according to SANS [16], it is one of the security assessment process phases. There are mainly two approaches to assess risk being qualitative and quantitative.

Qualitative risk assessment methods assign relative values to system risk, assets, consequences and countermeasures by identifying all the threats towards a system and its resources [25], [26]. This is achieved throughout conducting structured interviews, workshops and sending out questionnaires to security and system experts [25], [27]. Qualitative methods can be used to assess the relationship between threats and vulnerabilities [23].

Quantitative risk assessment methods assign numerical values to the likelihood, impact of the risk, and the costs and benefits of applying countermeasures [25]. These methods generally consider IS risk as a function of threat likelihood, and the expected loss caused by the threats targeting system vulnerabilities, they are also referred to as "expected value analyses" [28].

Figure 1 (taken from Paper C in this thesis) presents the relationship between qualitative and quantitative risk assessment and their differences, detailing the risk assessment process with regards to its resources, inputs, evaluation methods and outputs.

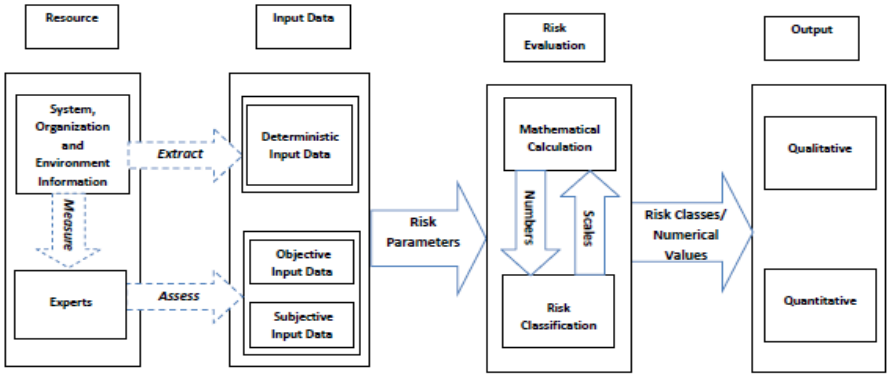

Figure 1, A Framework for Information System Risk Assessment

More details regarding the resources, input and actions are provided Section 3 and Paper C in this thesis. Regardless of the type of resources and input data, risk evaluation methods are categorized as being risk calculation (referred to as mathematical calculation in the paper) or risk classification. As shown in the figure, these two methods can be used in combination. For instance, by classifying inputs the risk classification approaches provide risk measure in terms of scale, and could be used as an input to risk calculation methods where the scales are transferred to numbers and vice versa.

2.2 Project Context

This section focuses on the research history and definitions within the project context. In general the overall process of project management is similar in most contexts. However, as previously discussed, activities and definitions may differ depending on the context where management and assessment is performed.

2.2.1 Project Management

There are various definitions for project management and its phases/activities depending on the domain where the project is conducted. The first international standard on project management was delivered in 2012 by ISO 21500 [29]. In 1996 the Project Management Institute (PMI) proposed the PMBOK guide [30], one of the most common definitions for project management. The PMBOK guide proposes guidelines for management of individual projects, and also defines project management related concepts, life cycle and its related processes. According to the PMBOK guide, project management activities can be categorized as follows.

Initiating*:* Activities that are performed to obtain authorization to start a new project or a new phase of an existing project.

***Planning**:* Activities that are performed to identify and define the scope of the project, the objectives, and the course of actions in order to achieve the project objectives.

***Executing**:* Activities that are performed to meet the project specifications that are defined in the project management plan.

***Monitoring and Controlling**:* Activities that are performed to review the progress and performance of the project; identify areas that a change of plan is required; and introduce the required changes in those areas.

***Closing**:* Activities that are performed to formally close the project by finalizing all the process group activities.

2.2.2 PROJECT ASSESSMENT

According to Davis [31] an assessment process is defined as a "systematic determination of the results of an effort or intervention". This process is assumed to enhance continuous improvement of project components. More specifically, project assessment is a process of investigating the project performance and deliverables, with a goal of identifying issues that cause deviation from the project plan defined in the initiation phase of project management to keep the project on track so as to maximize value for money and time invested in the project. One example of project assessment activities (shown in [32]) is as follows.

Clarify goals in measurable terms: Activities that are performed to translate the objectives and goals defined in the planning phase of project management process into measureable variables.

Develop strategies to measure the progress or outcomes: Activities that are performed to define representative indicators for project progress, success or failure. It is of value to identify key factors that affect the type of outcome the project leads to.

Identify the data required: Activities that are performed to gather all the information and data required for conducting analysis in order to evaluate the progress of the project or its outcomes.

Analyze data: Activities that are performed to analyze the collected data by considering the project plan and the measures that are enhanced by different sources such as statistical analysis, etc.

Improvement of the system: Activities that are performed to modify and improve the project outcome and progress by taking the results of the data analysis activities into account, which highlight the areas of project that need improvement.

2.2.3 PROJECT RISK MANAGEMENT

Disregarding contexts and roles, any action or decision taken by an individual introduces an unavoidable level of uncertainty and risk. In order to have a higher chance of making appropriate decisions, different sources of risk and uncertainty should be identified and addressed. By doing so, business managers, system designers and engineers will be assured that risk is either reduced by taking preventive actions such as applying security mechanisms

or is monitored and maintained at an acceptable level. If risk is not managed, the company or the individuals will face consequences ranging from human lives and injuries to monetary or trust loss. Therefore risk management is a critical process, which should be performed precisely according to standards and guidelines.

In this thesis, we apply a risk management process definition proposed by NIST 800-39 [33] and NIST 800-30[34], where risk management processes include the following phases, (i) framing risk; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk. Bellow we summarize each phase and its purposes.

The first phase establishes a risk context by describing the environment in which risk-based decisions are made. This activity enhances the organization to develop a strategy to assess risk, respond to risk and monitor risk [34].

The second phase addresses how organizations assess risk within the context of the organizational risk strategy set in the previous phase. The purpose is to identify threats to organizations, vulnerabilities internal and external to organizations, the harm; and the likelihood that harm will occur. This process results in a determination of risk, which typically is a function of the degree of harm and likelihood of harm occurring.

The third phase addresses how organizations respond to the risk that is determined by the risk assessment process. The purpose of this phase is to provide a consistent, organization-wide response to risk that is compatible with the organization risk strategy.

The fourth phase addresses how organizations monitor risk over time. The purpose of the risk-monitoring component is to determine the effectiveness and the implementation of risk responses; and satisfaction of information security requirements.

2.2.4 SOFTWARE DEVELOPMENT RISK MANAGEMENT

Failure to understand and resolve project risks can lead to a significant financial loss and even project failure, making it difficult for organizations to achieve their business objectives [35]. An example of such risky projects is software development. The reports on software projects' success statistics [36-38] indicate that as many as 9% [37] to 11.5% [36] of the projects are abandoned, aborted or cancelled. As software development failures put organizations at risk of substantial economic loss, it is critical for managers, stakeholders and developers to find solutions for prediction, assessment and management of undesirable situations that lead to failure in software development process. We refer to this process as *software development risk management*, where risk is "a particular aspect or property of software development task, process or environment, which, if it is ignored, will increase the likelihood of failure" [39].
As mentioned earlier one of the important phases of risk management is to respond to risk. Risk assessment and analysis lead to efficient risk response strategies that can obtain investor confidence [40]. Hall [41] introduced several risk response strategies, namely acceptance, avoidance, research, reduction and transfer [40]. For industry risk reduction is of particular interest as it can be achieved by risk mitigation, prevention or anticipation. Consequently, risk mitigation is one of the common approaches for evaluating and managing risk involved in different processes such as software development process.

2.3 SUMMARY

In this section we have given a brief description on the two main topics addressed by this thesis, namely security assessment and risk assessment. Because these topics vary in terminologies depending on context and setting, we have provided two separate in-depth overviews: one on security and risk assessment in the context of information systems, and one on risk assessment in the context of software development process. Moreover, we have shown there are similarities in the assessment process of security and risk, which leads to similar type of measures (qualitative and quantitative).

By reviewing research history in the field of information system security and risk assessment it becomes clear that there is a lack of practical and general approaches that could support managers and business owners with economic decisions. Such decisions could be about whether to invest on specific security functions or whether to perform thorough risk proofing for handling consequences of failure or fault occurrence at the organization or information system level. It is our belief that there is a tight connection between the management aspect of security/risk, and the more technical aspects of security/risk. As the concept of project management has been around long before management of information systems, we identify a need for researching both security and risk attributes from a management and information system perspective. We recognize management of the software development process as being a good case study as it involves assessment at management level as well as technical level. For this reason, we have chosen to highlight the process of risk management performed during development of software from two perspectives: the management perspective investigates each management phase while the technical perspective investigates each phase of the software development lifecycle. To that end, this thesis constitutes a summary of our research in security/risk assessment in information systems in general and the software development process in particular.

3. General Problem Statement and Summary of Research Contributions

The main objective of this thesis is to provide insights into the understanding of the security and risk assessment process performed within the two settings we mentioned in previous section namely, information systems and software development. Our work begins by introducing a model-based security-quantification approach for information systems. Applying the introduced model from the first paper in risk-assessment context, a modified version of one of the commonly used risk-analysis methods is proposed. One of our findings is that there seems to be a lack of clear exhibition of details in the risk assessment process. We therefore provide a framework/taxonomy that describes such details by categorization of key factors in the assessment process and provide a classification of risk-calculation methods. We also observe that security/risk assessment have major effects in making decisions by managers, and consequently believe that it is worth investigating these attributes from a management perspective as well. Moreover, we identify the software development process to be a good case as it involves both management and technical perspectives. Accordingly, we study the risk-management process within the process of agile and plan-driven development of software. Below we give a short description of each paper in terms of what research questions it addresses and what scientific contributions it makes.

The objective of the first paper (Paper A) is to provide a structured way for assessment and metrication of operational security. The paper contributes to the security metrication field by categorizing security metrics into two categories namely, *protective* and *behavioral* metrics. The paper considers integrity, a protective metric, as the most important aspect of security, and proposes a categorization of integrity metrics to *system-related* and *threat-related* metrics.

The objective of the second paper (Paper B) is to propose an approach for improving security risk calculation and analysis. The paper proposes an approach for improving reliability of one of the common risk-calculation methods by taking system operational factors into account. The paper introduces a measure called *probability of propagation*, which accounts for system operation, attack chain of impairment, and introduces a latency factor when calculating the probability of an undesirable event.

The objective of the third paper (Paper C) is to identify key players in the risk assessment process and their relationship. The paper proposes an abstract model or taxonomy of the risk assessment process with the goal of clarifying different phases involved in the assessment process. The contribution of this paper could be used as a base for development and investigation of new risk assessment methods.

The objective of the fourth paper (Paper D) is to investigate different strategies for risk management among various software development processes, primarily focusing on agile and plan-driven processes. The paper aims at validating the common belief of improved risk mitigation in agile development processes by conducting a Systematic Literature Review (SLR) on risk management through assessment of journal publications in the fields of software engineering, project, and risk management. The results can lead to well-established

decisions by developers and managers regarding the choice of a proper development model with better risk mitigation.

To summarize, the papers provided in this thesis are connected as follows: Paper A provides the base for Paper B by proposing a model-based security-assessment approach, which later in Paper B is applied to security-risk calculation. Moreover, while investigating risk assessment in Paper B, we realize a lack of clarity in information system-security risk-assessment process, which lead to our proposed framework in Paper C. In Paper C we investigate security-risk assessment in details, which clarifies a lack of practical and general approaches that can be applied by managers when faced with economic decisions. This leads to our investigation of the risk assessment presented in Paper D, which encompasses both management and technical perspectives of risk assessment.

3.1 Paper A: A Framework for Security Metrics Based on Operational System Attributes

There exist different approaches that measure specific attributes of security and dependability. However, to our knowledge, not many approaches exist that investigate the relation between such attributes and how they affect each other. Such information is valuable for designing more cost efficient, secure and reliable systems by guiding the designers to focus on the most important security and dependability attributes. Our work aims to simplify different measures of security and dependability, clarify their relation and propose a model to enhance development of new measurement methods. The main question *Paper A* addresses is ***which security and dependability attributes can be used to conduct operational system quantification?***

Furthermore, Paper A addresses the following questions:

- Is it possible to categorize operational security and dependability attributes based on their interaction with the system and environment?
- What is the relationship among these attributes?
- Is it possible to categorize different approaches that measure integrity?

Paper A is based on a conceptual (black box) model of a system and its interaction with the environment [45]. The model highlights the system detailed attributes, behavior, inputs and outputs to enhance metrication of dependability and security of the system of interest. It should be noted that the paper does not propose new attributes, but categorizes the existing ones based on the proposed conceptual model.

The contributions of Paper Aare as follows.

We categorize system operational security and dependability attributes as being either *protective or behavioral*. This categorization is based on the interaction of the system with the environment, its inputs, behavior and outputs. *Protective attributes* represent the system interaction with the input from the environment regardless of whether it is malicious or not. *Behavioral attributes* represent the system response to the input. This response could be delivery or denial of information or service, which is dependent on system attributes, and internal defense mechanisms such as recovery mechanisms.

We identify security and dependability attributes that can serve as metrics to quantify system operation in terms of protective and behavioral aspects. Identified protective attributes metrics are *integrity* (protecting the system from malicious input) and *accessibility* (possibility of accessing the system by authenticated users). Identified behavioral metrics are *confidentiality* (secrecy of information), *exclusivity* (secrecy of services), *availability* (readiness for correct service), *reliability* (full delivery or degraded delivery of service), and *safety* (absence of catastrophic failures).

We identify the relationship among protective and behavioral attributes based on system interaction with its environment. One important finding is that behavioral attributes are dependent on the protective ones. For instance, confidentiality and reliability of a system is dependent on integrity and accessibility of the system. This means the better the integrity and

accessibility are; the higher the chances are for a better confidentiality and/or reliability. As accessibility is a metric commonly used for normal input, it is possible to consider integrity as an essential aspect of security and dependability. This would help the designers to spend more time and money on improvement of integrity, which in turn would lead to a more secure system.

We categorize system integrity measurements as either being *system-related* or *threat-related*. *System-related approaches* measure integrity in terms of the system's ability to protect itself against malicious input. This could be calculated by for example measuring the combined strength of all involved security defense mechanisms, which are threat reduction, boundary protection and recovery. The *threat-related approaches* measure integrity in terms of the amount of effort an attacker has to expend in order to make an intrusion. The amount of effort could be calculated by assessing the attackers' skill level and the time spent for making an intrusion into a system. This categorization of integrity measurement approaches could help the designers to generate more structured approaches to test and metricate system security and dependability.

To summarize, Paper A investigates operational security and dependability metrics. The paper proposes a model-based approach to enhance categorization of operational security by taking environmental factors and system attributes into consideration.

3.2 Paper B: A Cause and Effect Approach Towards Risk Evaluation

In most approaches for system evaluation, risk assessment is a function of specific factors, such as threats and vulnerabilities. What is lacking in these methods is that they do not consider the probabilistic influence on risk from (1) system operation, (2) internal mechanisms and (3) the chain of system impairments. Indeed, other authors have suggested more refined risk analysis methods, such as probabilistic distribution among successful attacks [42] or calculating the effect of aggregating different tasks in a complex business process [43]. However, to our knowledge none of them has adopted a full input-output causal approach. The causal approach takes the system attributes and attack chain of impairments into account, improving the reliability of the probability calculation. One possible reason why this has previously not been done is that the probabilistic analysis becomes more complicated when considering the factors mentioned above. Our work presents a risk evaluation method that is more abstract and holistic than many other risk analysis methods that calculate risk. The main question *Paper B* addresses is ***how can the effect of system operation on the final security risk be calculated?*** Furthermore, Paper B investigates how to calculate risk when a threat leads to different types of system output.

Paper B proposes an improved version of commonly applied basic risk assessment formula, where risk is calculated based on probability of an unwanted event and the possible consequences of those events [44], [48]. Paper B is based on a previously proposed conceptual security and dependability model [45], which was also used in Paper A, in order to assess operational system security risk. The model enhances the probabilistic analysis by considering a so-called *causal chain of impairments.*

The contributions of Paper B are as follows.

We propose a risk assessment method that provides a clear explanation of the key factors in risk calculation, namely *system operation, attack chain of impairment, and latency* factor. The impacts of these factors are evaluated in terms of how they influence on system behavior and, in particular, system failure risk.

We suggest a new metric for calculating the risk probability called *probability of propagation*. To the best of our knowledge, this is the first attempt to apply the effects of the factors mentioned above and their impairments in risk calculation. Moreover, we propose a metric called *sum over probability of propagation and the related loss*. The purpose of this metric is to enhance capturing the different causal chains of impairment for a specific threat that leads to different types of outcomes. This is achieved by calculating each outcome with their respective probability of propagation and the consequences, so as to add up to a composite risk assessment.

To summarize, Paper B investigates operational security risk assessment. A novel factor, *probability of propagation*, is proposed to incorporate effects of system operation and chain of impairments into probability calculation of unwanted security events leading to some type of system failure.

3.3 Paper C: An Attempt to Structure Risk Assessment

Risk assessment is mainly used to identify threats and consequences of successful attacks and to prioritize the use of security resources in organizations [46]. There exist quite a number of risk assessment methods most of which focus on threat identification, vulnerability and asset assessment, probability and consequence calculation and final risk classification. Despite the existence of various risk assessment approaches, to our knowledge, certain matters remain unclear, for example type of information sources and data used for risk assessment, type of risk evaluation method and type of risk assessment process outputs. Our work makes an attempt to clarify these aspects. The main question *Paper C* addresses is ***if it is possible to categorize the risk assessment process with respect to the process inputs, internal evaluation methods and outputs.***

Accordingly, Paper C addresses the following questions:

- What are the types of resources required for this process and what type of actions are performed on them?
- What are the types of risk assessment inputs?
- What are different types of risk evaluation methods?
- What are different types of risk assessment outputs?

Paper C attempts to identify the main factors that play critical roles in risk assessment processes, how they are related to each other and what their effect is on the final risk. Thus, we put forward a structure/taxonomy attempting to clarify the uncertainties mentioned above as well as assessing the pros and cons of existing risk assessment methods. Further, we believe that this structure could provide a solid base towards development of new risk assessment methods.

The contributions of Paper C are as follows.

We categorize resources applied in risk assessment based on whether they are related to *system, organization and the environment* or related to *experts*. The first category refers to resources that can be applied to extract raw data required for the risk assessment process, such as logs of system vulnerabilities or summary of threats within a specific period. The *experts* category refers to resources that perform assessment and measurement over the first category and provide processed data, such as probability of launching an attack towards the system by an attacker.

We categorize risk assessment input as being *deterministic, objective* or *subjective*. The categorization is based on the type of resource and whether the action performed on resource is *extraction, measurement* or *assessment*. *Deterministic* inputs are produced by the mere extraction of data. In contrast, *objective* and *subjective* inputs are produced by measurement and assessment of data respectively.

We categorize risk evaluation methods as being *risk calculation (mathematical calculation)* or *risk classification*. The first category uses strict mathematical formulas and equations to calculate the risk. The second category classifies risk based on expert assessment of risk

parameters. We categorize *risk calculation* methods using approaches from different application domains.

- ***Cost benefit analysis*** uses either monetary gain (benefit) or monetary loss (cost) to assess risk.
- ***Game theory*** uses probability and consequences of different attack and defence scenarios taken by the players, and their utility functions to assess risk.
- ***Probabilistic risk assessment*** uses a 10-step process to identify initiating unwanted events that enhances modeling of different scenarios and their relevant system failures in terms of likelihood and severity.
- ***Uncertainty modeling*** uses three approaches being fuzzy, Monte Carlo or Analytical Hierarch Process to calculate the cognitive uncertainty factor involved in the risk assessment process.
- ***Supplementary approaches*** such as Markov modeling or matrix-based approaches that are commonly used in combination with other mathematical calculation methods to enhance probability and consequence calculation.

We categorize risk assessment outputs to *qualitative* and *quantitative* representation of risk. The *qualitative* outputs describe risk in terms of scales and words. However, *quantitative* outputs represent risk by numbers assigned to risk.

To summarize, Paper C investigates the process of information system risk assessment. The paper proposes an outline for enhancement of the risk assessment process by clarifying different phases of the assessment process, types of inputs and outputs of these phases and different types of risk evaluation methods.

3.4 Paper D: Systematic Literature Review on Risk Management in Plan-driven and Agile Software Development

It is commonly believed that companies in the software development industry assume that risk management and mitigation is better in projects that adopt agile processes than in projects where plan-driven processes are adopted. An explanation for this could be that risk mitigation and resolution is performed earlier in agile process. However, the validity of this belief has never been thoroughly investigated. To investigate whether this is indeed the case, there is a need to compile existing research and practices on risk management. Our work contributes to this through a systematic literature review (SLR) that summarizes existing empirical evidence on risk management collected from journal publications in the fields of software engineering, project management and risk management. The main question Paper D addresses is ***if risk mitigation is affected by the choice of the development process.***

The review was conducted in the fields of software engineering, project management and risk management. Using a set of rigorous inclusion and exclusion criteria, 78 primary studies were selected.

The contributions of paper D are as follows.

We show that there exist no publications that report a difference in risk mitigation between agile and traditional development approaches. This is surprising given the common belief. We identify a broad set of application domains that are investigated by the existing research as being defense, financial sector, information systems, medical industry, telecom, space, Enterprise Resource Planning and automation. Among this broad set of domains only three (defense, financial sector and information systems) are addressed by more than two primary studies.

We categorize the research methods as being *empirical* or *non-empirical*. The *empirical research methods* found are *case study, survey, controlled experiment* and *action research*. The *non-empirical research methods* found are design of *models* and *theoretical research methods.* We found that the most applied research method is design of models, being addressed by as many as 49 primary studies.

We identify the types of risk investigated in research being *perceived* or *actual risk*. We find that the most common type of risk is perceived risk being addressed by 41 primary studies. We have also identified *Requirement analysis phase* and *planning phase* being the most addressed development and management phases, addressed by 18 and 23 primary studies respectively.

To conclude, the major findings of this review is that there is lack of clarity regarding application domains among research papers in this filed. 62 out of 78 studies did not have clear descriptions of neither the domains where the study was performed in nor the domain it could be applicable to. This is essential to be addressed to enable academics to investigate the generality of a domain specific model in other domains, and providing guidelines for industry when adopting domain-specific models or methods.

There is lack of validity and limitation investigations among research papers in this filed. Although, more than half of the primary studies (49 publications) are categorized as design of models, limitations and threats to validity of proposed models are only addressed by 19

publications. Accordingly, 30 out of 49 publications have no validity check leading to low rank for these publications when assessed by our quality assessment system.

There is also lack of clarity regarding the development models. Among 78 primary studies, 66% did not have clear descriptions of the development models. Although we did not limit our SLR to any specific models, this could have led to missing more than half of the primary studies. Accordingly, it is hard to review the literature regarding trends in any specific development models.

There is lack of quantitative risk assessment studies in this filed. By conducting this review, we found out not many quantitative empirical studies have been performed in different domains. However, these studied could lead to valuable data beneficial for academics and industry.

Furthermore, there is lack of general SLRs among research papers in this filed. To the best of our knowledge, the existing SLRs have thorough inclusion/exclusion of criteria focused on very specific aspects of software engineering and/or risk management such as global software development or eXtreme programming. Therefore, we believe there is a need to highlight a demand for empirical research on risk management applied in different development models and domains.

Finally, there is lack of empirical investigations of the superiority of agile process with regard to risk mitigation among research papers in this filed. Even if this assumption is true, we neither found any empirical evidence proving better risk mitigation in agile processes, nor any papers investigating the possible gap between risk mitigation in agile and plan-driven approaches.

To summarize, Paper D investigates software development risk management. The paper investigates a software development process with respect to the development lifecycle phases among different software development models specifically agile and plan driven. Moreover, the paper treats a software development process as a project and investigates the management phases of this project.

The results of this review encourage further empirical investigation of risk management in different software development models. Studies like the one performed provide a classification of models, their advantages, and challenges enabling software project managers to make decisions that would improve companies' return on investment and reduce the number of abandoned or failed software development projects.

4. CONCLUSION

In today's IT industry a business is as successful as its security and risk management. The more complex the IT solutions are the harder it is to figure out which parts of the system are more prone to failure in terms of service due to security vulnerabilities. On a daily basis managers need to make economic decisions about actions that must be taken in order to keep the business running without spending too much time and money. Accordingly, these decisions need to be taken based on information provided by the technical divisions of the company. In most cases it is not an easy task to translate technical information to a relevant management question; therefore, there is a need for a common language, or factor, that both parties can connect to. We believe that factor is risk. More specifically, we believe that a terminology for risk can be adopted both by security experts, to assess the probability of a threat attacking a system vulnerability will cause a system failure, as well as by managers, to assess how probable it is that a project will exceed the budget or deadline.

This thesis comprises a study of operational security and risk assessment in information systems in general, taking a black box approach. To that end, the thesis presents an investigation of risk assessment and management in a more special setting, namely the software development process. However, as this thesis addresses different features of information systems, it also attempts to clarify different terminologies within the two contexts.

Our work begins by investigating dependability and security attributes by applying a preexisting back box model of system operation to categorize and identify metrics that provide a good insight into system security and dependability. One finding from Paper A is that the system operation and defense mechanisms have a significant effect on the system output. Based on this, we decide to apply this concept in security risk-calculation by proposing a possible improvement taking system chain of impairments into account in Paper B. While investigating security risk calculation and assessment, we review proposed qualitative and quantitative approaches and find that they are not relevant to apply, as they do not have a clear view of the parameters they used for the assessment process. This leads to the proposed taxonomy that is presented in Paper C. As we realize that risk assessment is a young field within the area of information-system security, we also investigate this process within an older field, namely software development. The results from a systematic literature review investigating risk assessment in software development are presented in Paper D.

Below we summarize the main results presented in this thesis and highlight the contributions of this research.

4.1 SUMMARY OF RESULTS AND CONTRIBUTIONS

The main research result of this thesis is that it highlights the lack of clarity and consistency regarding definitions and terminologies, by providing an insight towards the understanding of the security and risk assessment process performed within two important settings, namely information systems and software development. To that end, the thesis proposes a categorization of a set of attributes to be applied as metrics for quantifying operational system security. Moreover, by highlighting system operation and internal mechanisms effect on

system output, the thesis proposes a new metric for calculating risk probability. Further, the thesis proposes a structure that clarifies the resources, inputs, evaluation method and outputs involved in qualitative and quantitative risk assessment process. Finally, to provide a wider view the thesis investigates how risk is assessed and managed in a bigger setting, in the context of software development.

This thesis makes some detailed contributions, which we believe puts the focus on some research questions and areas that have not been thoroughly investigated. We conclude this thesis by summarizing these contributions.

- Proposing a model-based approach that enhances categorization of operational security by taking environmental factors and system attributes into consideration.

- Identifying system operational security and dependability attributes as being either protective or behavioral.

- Identifying integrity and accessibility as protective attributes metrics.

- Identifying confidentiality, exclusivity, availability, reliability, and safety as behavioral attributes metrics.

- Identifying that behavioral attributes are dependent on the protective ones.

- Proposing that integrity should be the main system operation attribute that is required to be measured.

- Proposing that system integrity measurements can be categorized as being either being system-related or threat-related.

- Proposing a novel factor to incorporate effects of system operation and chain of impairments into probability calculation while assessing security risk.

- Proposing an outline to enhance the risk assessment process by identifying the phases of the process.

- Proposing a categorization for resources, inputs, evaluation methods and outputs of the risk assessment process.

- Proposing a categorization for different types of risk calculation methods.

- Highlighting research performed on risk assessment from a project management and software development perspective.

- Clarifying that there is no evidence published regarding improvement of risk mitigation and management in agile development, which hopefully will enable software project managers to make more informed decisions that would increase the amount of successful software development projects.

- Proposing a categorization of research methods as being empirical or non-empirical and the types of risk investigated in research being perceived or actual risk.

4.2 FINAL COMMENTS

We believe this thesis highlights the connection among different measures namely, security, dependability and risk within three contexts and research fields namely information system security, software development and project management. This could lead to adaption of new or currently existing approaches for measurement, mitigation, or handling of risk and security from one filed to another. One example of this adaption was presented by this thesis where the same model for security metrication was applied to show the effect of system operation on probability calculation while assessing risk. This highlights the connection between the two fields of risk and security measurement in Information systems. Another example this thesis highlighted is where software development risk is addressed from a project perspective where risk in requirement engineering was identified to be tightly connected to risk involved in planning and initiation phase of project management. Therefore, similar approaches that are applied for mitigation of risk in early phases of project cycle can be applied for risk in requirement engineering.

We believe the results show that there is a need for further investigation of different types of risk, and their calculation and management approaches within common fields such as information system, project management, and cognitive behavior psychology.

REFERENCES

[1] Avižienis A, Laprie JC, Randell B, Landwehr C., "Basic concepts and taxonomy of dependable and secure computing", Dependable and Secure Computing, IEEE Transactions, 2004 Jan, 11-33.

[2] J.C. Laprie, "Dependability: Basic Concepts and Terminology", ed., Springer-Verlag, 1992.

[3] Sun, L., Srivastava, R., Mock, T., "An information systems security risk assessment model under the Dempster–Shafer theory of belief functions", Journal of Management Information Systems, (2006) 109–42.

[4] ITSEC, "Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonized Criteria", Commission of the European Communities: COM (90) 314, Version 1.2., June 1991

[5] Common Criteria. ISO/IEC 15408-1, Information Technology- Security Techniques - Evaluation Criteria for IT Security, Part 1: Introduction and General Model, 1999.

[6] Wyss, G.D.; Clem, J.F.; Darby, J.L.; Dunphy-Guzman, K.; Hinton, J.P.; Mitchiner, K.W.; "Risk-based cost-benefit analysis for security assessment problems", Security Technology (ICCST), 2010 IEEE International Carnahan Conference on, vol., no., pp.286-295, 5-8 Oct. 2010

[7] Talbot, Julian. and Jakeman, Miles. Risk Management Institution of Australasia. "SRMBOK: security risk management body of knowledge" ,Carlton South, Vic 2008

[8] P.G. Neumann, Computer Related Risks. ACM Press and Addison-Wesley, New York, 1995.

[9] "Art, n.1." OED Online. Oxford University Press, June 2015. Web. 8 September 2015.

[10] Alex Dali, Christopher Lajtha, ISO 31000 Risk Management, "The gold Standard", EDPACS, Vol. 45, No. 5, 2012

[11] ISO 26261-2011, "Road vehicle- Functional safety": Part 1 to 9, November 2011

[12] Control Objective for Information and related Technology (COBIT) 4th Edition; published by Information System Audit and Control Association (ISACA)

[13] R. Khan, "Practical Approaches to Organizational Information Security Management", SANS Institute, 2010

[14] ISO/IEC 17799/27002 Information Technology Security Metrics, Code of Practice for Information Security Management, published by International Standardization Organization (ISO).

[15] J. Ropponen, K. Lyytinen. (2000), “Components of software development risk: how to address them? A project manager survey”, IEEE Transactions on Software Engineering, 26(2), 98–112

[16] Craig S. Wright, “A taxonomy of information system audits, assessment and reviews”, SANS Institute, 2007

[17] Henning, R. et al. Proc. of Workshop on Information Security System, Scoring and Ranking, ACSA and MITRE, Williamsburg, Virginia, May 2001

[18] RB Vaughn Jr, R Henning, A Siraj, “Information assurance measures and metrics-state of practice and proposed taxonomy”, Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 2003.

[19] National Institute of Standards and Technology Special Publication 800-55, “Performance Measurement Guide for Information Security”, July 2008

[20] National Institute of Standards and Technology Special Publication 800-26, “Security Self-Assessment Guide for Information Technology Systems”, Nov 2001

[21] N. Seddigh, P. Pieda, A. Matrawy, B. Nandy, I. Lambadaris, A. Hatfield, “Current Trends and Advances in Information Assurance Metrics”. Proc. of the 2nd Ann. Conf. Privacy, Security and Trust (PST 2004), Fredericton, NB, Oct 2004.

[22] Mike Kleckner, “Facilitating the quality of security assessment: overview of the process of defining and delivering security requirements for application systems”, SANS Institute, 2001

[23] Jaisingh, J. and Rees, J., “Value at risk: A methodology for information security risk assessment”, In Proceedings of the INFORMS Conference on Information Systems and Technology (Miami, Nov. 3--4, 2001).

[24] Butler, S., “Security Attribute Evaluation Method: A Cost Benefit Approach”, Proc. 24th Int’l Conf. Software Eng. (ICSE 02), IEEE CS Press (2002) 232–240

[25] Bojanc, K., Jerman-Blažič.B, “An economic modelling approach to information security risk management”, International Journal of Information Management, 28 (5), (2008) 413-422

[26] Mosleh, A., Richard Hilton,E., S. Browne,P.: “Bayesian probabilistic risk analysis”, ACM SIGMETRICS Performance Evaluation Review, vol.13, No.1,(1985) 5-12

[27] Wang, Z., Zeng, H., “Study on the risk assessment quantitative method of information security”, Advanced Computer Theory and Engineering (ICACTE), vol.6, (2010) 529 – 533

[28] Sun, L., Srivastava, R., Mock, T., “An information systems security risk assessment model under the Dempster–Shafer theory of belief functions”, Journal of Management Information Systems, (2006) 109–42.

[29] ISO 21500-2012, “Guidance on project management”, September 2012

[30] Project Management Institute, “A Guide to the Project Management Body of Knowledge” (PMBOK Guide), Newtown Square, Pa: Project Management Institute, 2004

[31] Dr. Josephine D. Davis, “Project assessment and evaluation plans”, presented for quality education for minorities, Canada, 2010

[32] The Duke Center of Instructional Technology.

Available: https://cit.duke.edu

[33] National Institute of Standards and Technology Special Publication 800-39, “Managing Information Security Risk Organization, Mission, and Information System View”, March 2011

[34] National Institute of Standards and Technology Special Publication 800-30, “Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology”, July 2012

[35] J.M. Verner, L.M. Abdullah, “Exploratory case study research: outsourced project failure”, Information and Software Technology, 866–886.

[36] El Emam, K. and Koru, G., (2008), “A replicated survey of IT software project failures”, EEE Software, 85-90.

[37] Sauer, C., Gemino, A. and Reich, B. H. . (2007), "The impact of size and volatility - On IT project performance", Communications of the Acm, 50(11), 79-84.

[38] Tichy, L. and Bascom, T. (2008), “The business end of IT project failure Mortage Banking”, 68(6), 28.

[39] J. Ropponen, K. Lyytinen. (2000), “Components of software development risk: how to address them? A project manager survey”, IEEE Transactions on Software Engineering, 26(2), 98–112

[40] Wiemann, P, “Risk management and resolution strategies for established and novel technologies in the low head”, 2011

[41] Hall. E, “Methods for Software System Development”, Addison-Welsey, 1997

[42] R. Breu, F. InnerhoferOberperfler, A.Yautsiukhin, “Quantitative assessment of enterprise security system,” ARES’08 Proceedings of the 2008 Third International Conference on Availability, Reliability and Security, pp.921-928, 2008

[43] F.Massacci, A. Yautsiukhin, “Modelling Quality of Protection in Outsourced Business Processes”, In Proc. of IAS'07, IEEE Press 2007

[44] U.S. Department of Homeland Security Risk Steering Committee, “Risk Lexicon,” U.S. Department of Homeland Security, Washington, DC., September 2008.

[45] E. Jonsson, “Towards an integrated conceptual model of security and dependability”, The First International Conference on Availability, Reliability and Security, 2006, ARES 2006, vol., no., pp. 8 pp., 20-22 April 2006.

[46] Butler, S., “Security Attribute Evaluation Method: A Cost Benefit Approach”, Proc. 24th Int’l Conf. Software Eng. (ICSE 02), IEEE CS Press (2002) 232–240.

[47] European Telecommunications Standards Institute, TS 102 165-1 V4.2.3, TISPAN, Methods and Protocols; Part 1 Method and Proforma for Threat, Vulnerability Analysis, 2010-2012.

Available: http://www.etsi.org

[48] S. Kaplan, and B.J. Garrick, “On the Quantitative Definition of Risk,” Risk Analysis, vol. 1, No.1, pp.11-27, 1981

Appended Papers

Paper A: *Identifying Suitable Attributes for Security and Dependabiliy Metrication*

Erland Jonsson, Laleh Pirzadeh

SECUREWARE 2013, the 7th International Conference on Emerging Security Information, Systems and Technologies, Barcelona, 25-31 August, 2013

Paper B: *A Cause and Effect Approach Towards Risk Analysis*

Laleh Pirzadeh, Erland Jonsson

Metrisec 2011, Third International Workshop on Security Measurement and Metrication, Banf, 20-21 September, 2011

Paper C: *An Attempt to Structure Risk Assessment*

Laleh Pirzadeh

Nordsec 2012, The 17th Conference on Secure IT Systems, Karlskrona, Sweden, 31 October-2 November, 2012

Paper D: *A Systematic Literature Review on Risk Management in Agile and Plan-driven Software Development*

Laleh Pirzadeh, Ana Magazinus, Richard Torkar

Technical report 2016:06, ISSN: 1652-926X