A Quantitative Risk Analysis Approach for Deliberate Threats

Nikos Vavoulas, Christos Xenakis

Department of Digital Systems, University of Piraeus, Greece
nikos.va@gmail.com, xenakis@unipi.gr

Abstract. Recently, organizations around the world are becoming aware of the need to run risk management programs in order to enhance their information security. However, the majority of the existing qualitative/empirical methods fail to adhere to the terminology defined by ISO 27000-series and treat deliberate threats in a misleading way. In this paper, a quantitative risk analysis approach for deliberate threats is introduced. The proposed approach follows the steps suggested by the ISO 27005 standard for risk management, extending them in order to focus on deliberate threats and the different information security incidents that realize them. It is based on three-levels: the conceptual foundation level, the modeling tools level and the mathematical foundation level. The conceptual foundation level defines and analyzes the terminology involved, using unified modeling language (UML) class diagrams. The modeling tools level introduces certain tools that assist in modeling the relations among different concepts. Finally, the mathematical foundation level includes all the different mathematical formulas and techniques used to estimate risk values for each threat.

Keywords: risk analysis, quantitative, deliberate threat, risk estimation, risk identification.

1 Introduction

More and more organizations around the world are becoming aware of the need to run a risk management program in order to enhance their information security. *Risk management* includes coordinated activities to direct and control an organization with regard to risk [3][4]. Standardization organizations, such as NIST (National Institute of Standards and Technology) and ISO (International Organization for Standardization), have issued risk management guides [5][6], in an attempt to create a common language, providing both the definitions and the practical guidance necessary for assessing and mitigating risks related to potential information security incidents, identified within Information Technology (IT) systems. An information security incident is a single or a series of unwanted or unexpected information security events, which have a significant probability of compromising business operations and threatening information security. On the other hand, an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant [9].

A risk may arise through three different kinds of threats: environmental, accidental or deliberate. The risk related to environmental and accidental threats in most cases, can be adequately described by empirical/qualitative data. However, the same data may not be able to describe adequately the risk related to deliberate threats. IT systems operate in a menacing environment that constantly changes and thus past data may not necessarily describe a present situation. Things may become even worse when dealing with threats that are realized through technological vulnerability exploitation. New vulnerabilities are discovered in a daily basis in both hardware and software, allowing new attacks, with no previous of occurrence and thus limited or zero data about them. CERT (Computer Emergency Response Team) has catalogued over 21000 vulnerabilities from 2006 to 2008 [7]. Moreover, older vulnerabilities may become easier to exploit through time, since technology advances and becomes cheaper or implemented controls are becoming inefficient. Finally, empirical data and attack statistics are scarce [8], since organizations are reluctant to publish information regarding the attacks on their systems, for fear that the same or similar vulnerability will be exploited by other attackers, or for fear of suffering reputational damage.

Deliberate threats also differ from the other two threat categories (i.e., environmental and accidental) as it is the only threat category, which involves a specific type of information security events: the attacks. Each attack is related with a different probability of occurrence and consequence value, and thus, a different risk value. In many cases a single threat is realized by launching more than one attacks. Therefore, in order to estimate the risk of a deliberate threat, all different attacks, attacks series and the relations among them should be examined. Deliberate threats are complicated by nature, with many unforeseen aspects and thus should be elaborated in details in order to get full results from the risk analysis process. All the above mentioned issues clearly show the need to develop and adopt quantitative risk analysis methods which can be used either as stand-alone methods or as enhancements to the current methods that use qualitative/empirical data.

In this work, an in-depth quantitative risk analysis approach for deliberate threats is introduced. The proposed approach follows the steps suggested by ISO 27005 standard for risk management [5], extending them in order to focus on deliberate threats and the different information security incidents that realize them. It is based on three-levels: the conceptual foundation level, the modeling tools level and the mathematical foundation level. The conceptual foundation level is achieved by using class diagrams of the unified modeling language (UML) that follow the risk analysis terminology defined in ISO 27005 [5]. This level is further facilitated by the modeling tools and the mathematical foundation level. The proposed modeling tools help in modeling conceptually the relations among different concepts. Finally, the mathematical foundation level includes all the different mathematical formulas and techniques used to estimate risk values for each threat.

The remainder of this work is organized as follows: Section 2 discusses the limitations of current risk analysis approaches that motivate this work. Section 3 presents the conceptual and mathematical background that this approach is based on, as well as the tools that uses. In section 4 the entire approach is described, step-by-step, while section 5 provides a theoretical example of this. Finally, section 6 outlines the conclusions and future work.

2 Motivation

ISO 27005 [5] is a standard of the ISO 27000-series concerning information security risk management. It includes definitions about the main concepts involved in risk management, as well as a detailed description of the processes involved. According to ISO 27005, risk analysis is a group of two distinct processes that are involved in risk management: risk identification and risk estimation. Risk identification is the process where the unwanted events that may cause potential loss are determined. On the other hand, risk estimation is the process where qualitative or quantitative values concerning the probability and the consequences of the identified events are assigned. ISO 27005 describes generically all the steps required to perform a risk analysis but it does not propose any specific qualitative or quantitative risk analysis approach.

Currently, there are several qualitative risk analysis approaches/methods such as CRAMM, CORAS, OCTAVE, FRAP etc., some of which are widely used. Most of these methods are either incompatible or partially compatible with ISO 27000-series in terms of the conceptual foundation, the results and the steps that should be followed in risk analysis, since some of these methods pre-existed ISO 27000-series and its ancestors (i.e. BS 7799 part one and part two). CRAMM is one of the oldest risk analysis methods, which lately has incorporated an add-on in its supporting tool (version 5) [10] that it maps the suggested countermeasures with the ISO 27001 and ISO 27002 suggested controls. However, CRAMM still remains incompatible with ISO 27000-series since it uses terms, such as risk management, with completely different meaning. The entire set of available risk analysis methods (i.e., including CRAMM) considers different types of threats using the same processing steps and a certain level of details. This can be proved misleading for deliberate threats, which usually present an elevated level of complexity (i.e. dependence among attack events, different threat-source capabilities etc.). Moreover, some of most widely used risk analysis methods focus on the business perspective regarding risk. However, in deliberate threats, attackers' perspective is also important, since what the organization wants to protect not necessarily identifies with what a malicious can/wants to attack. Furthermore, qualitative approaches do not provide a basis for a cost-benefit analysis making difficult to justify investments in control implementation.

Recently, a few quantitative risk analysis approaches have been proposed, that try to address some of the limitations of the aforementioned methods. Zaobin Gal et al. have presented a risk estimation methodology for information systems [11], which introduces a "through the eyes of the adversary" approach. In this work, they propose the use of an extended version of the Shneier's attack trees [1, 2]. An attack tree represents the attacks that realize a threat as a tree structure. The root node represents the goal of the attack, while the leaf nodes represent the different attacks needed in order to accomplish the goal. The extended version of attack trees covers the case of attacks launched under the condition that other attack(s) preceded. Another study that focuses on the risk assessment of VoIP call interception [12], proposes a formal risk assessment method, which includes two modeling techniques: attack trees and vulnerability dependency graphs. While attack trees are used to model the threat under examination (VoIP call interception), the vulnerability dependency graphs present the dependencies among the identified vulnerabilities and how these vulnerabilities interact to each other. Although, both of the quantitative approaches mentioned above provide an in-depth level of risk analysis for deliberate threats, they are attacker driven only, focusing on the probability of a vulnerability being exploited rather than the consequences that an organization would suffer. Furthermore, there are no ISO-compatible, limiting their use, and do not consider multiple attacker profiles. However, some of the ideas proposed in these approaches are adopted, extended and optimized in this work, in an attempt to make some steps towards a risk analysis method for deliberate threats, free of the limitations and deficiencies mentioned above.

3 Proposed Approach

The proposed risk analysis approach for deliberate threats consists of three distinct levels of details (see figure 1). The highest is the conceptual foundation level, which defines and analyzes the terminology involved using UML class diagrams. The intermediate is the modeling tools level, which introduces certain tools that help in modeling conceptually the relations among different concepts. Finally, the bottom level is the mathematical foundation level, which includes all the different mathematical formulas and techniques used to estimate risk values for each threat.

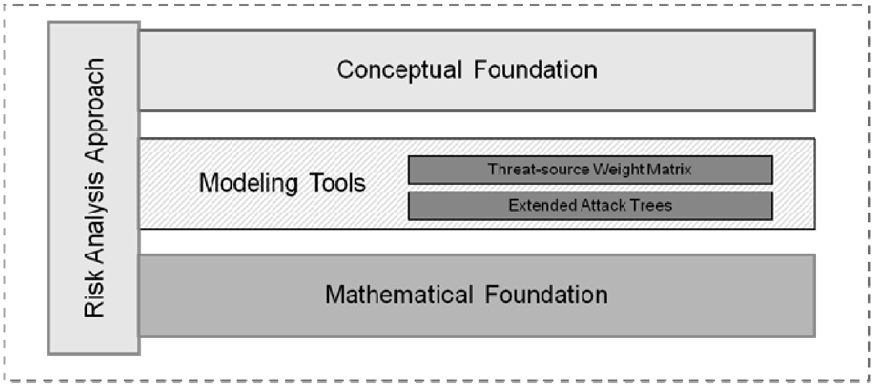

Fig. 1. The proposed three-level risk analysis approach

3.1 Conceptual Foundation

The conceptual foundation level achieves concept formalization using UML class diagrams [13]. The latter present, formally, how different concepts, involved in risk analysis, are related and which attributes of each concept participate in the risk estimation process. In order to create these diagrams, the concepts involved in the proposed risk analysis approach for deliberate threats should be identified and defined.

As mentioned previously, ISO 27005 classifies threats into three main categories: deliberate, accidental and environmental. Each of these categories is directly related to a set of concepts involved in a risk analysis process. An exception is the deliberate threats, which are related to an extra concept; the concept of "attack" (see Table 1). In the following, the concepts that are involved in the proposed risk analysis approach for deliberate threats, are defined according to the ISO 27000-series:

Table 1. Concepts related with different threat categories

	Environmental	Accidental	Deliberate
Asset	✓	✓	✓
Risk	✓	✓	✓
Vulnerability	✓	✓	✓
Threat-source	✓	✓	✓
Attack	✗	✗	✓

- Asset is "anything that has value to the organization" and which therefore requires protection.
- Threat is the potential cause of an unwanted event (i.e., an attack), which may result in harm of a system or organization.
- Vulnerability is a weakness of an asset or control (i.e., in ISO 27000-series, a control is a synonym of a countermeasure), which may be exploited by a threat. This general definition covers all threats categories. However, for deliberate threats, vulnerability is a weakness of an asset or control, which may be exploited by an attack to realize a threat.
- Risk is the combination of the probability of an event and its consequence.
- Attack is an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
- Threat-source is anyone whose intention is to exploit an asset's vulnerability, launching an attack and thus, realizing a threat. Threat-source is a synonym of an attacker.

Figure 2, presents the UML class diagram of the concepts defined above using three different types of relations: association, aggregation and composition [13]. Association is represented with a simple line between two classes and denotes a simple relationship between two classes. Aggregation is represented with a transparent diamond shape and denotes a part-whole or part-of relationship between two classes. Finally, composition is represented with a solid diamond shape and denotes a strong life-death relationship between classes. Notation at the ends of each relation in the diagram is called multiplicity and indicates the number of objects that participate in the relation. For example, in figure 2 we can see that a threat may harm one or more (1…*) assets. On the other hand, an asset might be at risk by zero or more threats (0…*).

As illustrated in the UML diagram, deliberate threats are realized through information security incidents which involve the occurrence of one or more attacks. The latter exploit one or more of the asset's vulnerabilities to realize threats, and thus, harm the assets. The self-association of the attack class represents attacks series (i.e., a sequence of attacks) realizing one or more threats. Attack series may be either dependent events (i.e., occurrence of one affects occurrence of another) or independent events (i.e., occurrence of one does not affect occurrence of another).

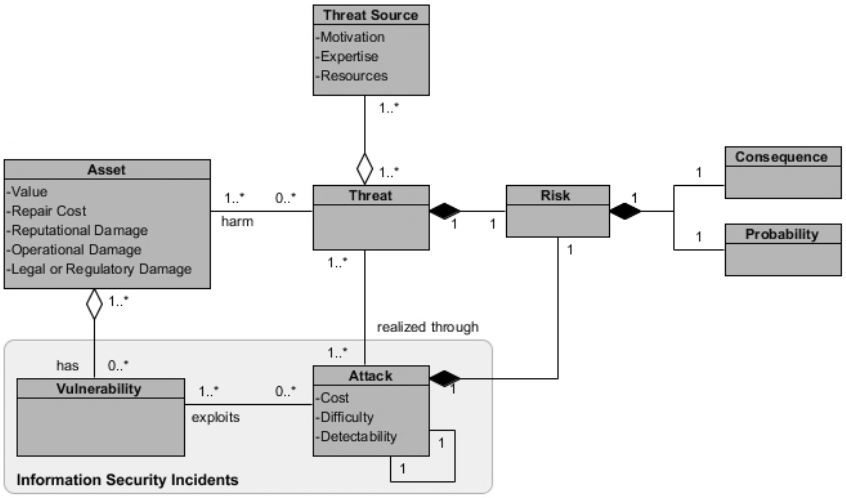

Fig. 2. UML class diagram for the proposed risk analysis approach

A threat may harm one or more assets and is related with one or more threat-sources. The aggregation relation between these two classes (i.e., threat and threat-source) denotes that if a threat is removed, then the same threat-sources may still exist for other threats. The risk analysis process estimates a risk value for each identified threat. This value is related to the probability of each threat to be realized and the corresponding consequences that occur. As mentioned previously, deliberate threats may be realized through one or more attacks, each of which has its own probability of occurrence and consequences, and, thus, its own risk value (Figure 2). The estimated risk value of a threat equals to the maximum risk value of all single attacks or series of attacks, which realize the threat. Consequently, risk values of the identified attacks and series of attacks should be estimated prior to estimating the risk value of the related threat. Since each threat is related with a unique risk value, if this threat is removed, then the corresponding risk value no longer exists. To represent this life-death dependency between the threat class and the risk class, as well as between the risk class and the attack class, the composition relation is employed.

Each of the concepts identified and modeled formally using the UML class diagrams, has certain attributes that should be considered during the risk estimation process. Some of these attributes are related to the probability of occurrence of a threat; while others are related to the consequences following the threat occurrence. However, not all of these attributes are always relevant with the threat under examination, and thus, each case should be studied separately. The attributes, which are included in the modeled concepts of the proposed approach and consider both business and attackers' perspectives, are:

- Threat-source
  - Motivation: what motivates a particular threat-source (or attacker) to launch an attack.
  - Expertise: the level of knowledge of a particular threat-source (or attacker) related to an attack.
  - Resources: the resources (money, equipment) that a particular threat-source (or attacker) has in its possession.
- Attack
  - Cost: the cost of equipment needed to launch an attack.
  - Difficulty: the level of expertise needed for someone to launch an attack.
  - Detectability: the easiness or difficulty of an attack being detected.
- Asset
  - Value: the value of a specific asset (it may also be considered as the cost of replacement).
  - Repair Cost: the cost to repair an asset.
  - Reputational Damage: the damage in reputation occurs if an asset is compromised.
  - Operational Damage: the damage occurs in an organization's or system's operation due to the compromised asset.
  - Legal and Regulatory Damage: the fines and penalties that will be paid because of the compromised asset.

3.2 The Modeling Tools

The modeling tools used in the proposed risk analysis include: (i) the threat-source profile matrix and (ii) the extended attack trees. The chosen tools link the conceptual with the mathematical foundation level of the proposed approach, as explained bellow.

The Threat-source Profile Matrix. The threat-source profile matrix is a two-dimensional matrix, which contains the weights of the attributes involved in an attack probability estimation (i.e. cost, difficulty, detectability) for all different threat-sources. The UML class diagram of Section 3.1, shows that a threat is related with one or more threat-sources. Each threat-source has each own motivation, resources and expertise level and thus there is a different probability for each threat-source exercising a specific attack. For example, the high cost of an attack wouldn't be for a professional hacker as deterrent as it would be for a script kiddy. In other words, while the cost attribute does not carry too much weight in the attack probability estimation for a professional hacker, it does for script kiddies which have limited resources. In order to reflect this diversity in probability values for different threat sources, profiles are created by assigning weight values for each attribute taking part in an attack probability estimation.

The Extended Attack Trees. Attack Trees [1] [2] represent a formal method of representing the varying of attacks that a system is exposed to, using a tree structure. The root node of the tree symbolize an identified threat, while the leaf nodes stand for the information security events (single attacks or attacks series) that realize the specific threat. The intermediate nodes of the tree can be either alternative subgoals, each one satisfying the parent goal (OR Nodes), or partial subgoals, whose composition satisfies the parent goal (AND Nodes). In a compound system there are several threats and consequently, attack trees, which form an attack forest. Attack trees can be illustrated both graphically and textually. However, graphical representation is not appropriate for composite systems, due to the enormous size that the tree could reach. In the proposed risk analysis approach, an extended version of the attack trees [11], which incorporates the CAND (Conditional AND) node is used. The classic attack trees cannot formally represent all the previously described information security incidents. Although the AND nodes of a tree can be used for depicting attacks series of independent events, they cannot be used for attacks series of dependent events, where the attacks occur under certain occurrence conditions. This is achieved by adding the CAND node (i.e., extended attacks trees). The CAND relation between nodes represent that the upper node is accomplished if all sub-nodes are attained under certain conditions.

3.3 Mathematical Foundation

As mentioned previously, the risk is the combination of the probability of an attack event and its consequences. In this approach, the risk value of an attack is derived by multiplying the probability of occurrence value of the attack with the estimated consequences, as shown in equation (1):

$$Risk(Attack) = P(Attack) \times C(Attack) \quad (1).$$

In order to estimate the attack probability value, utility curves from the multi-attribute utility theory are adopted that convert the attribute values into utilities. In the current approach, the utility curve chosen is the $U(x) = \frac{1}{x}$. We chose this utility function because the probability attributes are in inverse proportion with the probability itself. Furthermore, it can accurately represent residual risk as the probability can never become equal to zero. Risk can only become equal to zero if the consequences are equal to zero or the corresponding vulnerability is removed. Each utility is then multiplied by the corresponding weight of the threat-source under examination and summed up to the probability value, as shown in equation (2):

$$P(Attack) = W_{cost} \times U(cost) + W_{diff} \times U(diff) + W_{dete} \times U(dete) \; (2),$$

Where:
cost = Cost of an attack,
diff = Difficulty of an attack,
dete= Detectability of an attack,
Wcost = weight of the attack cost for a specific threat-source,
Wdiff = weight of the attack difficulty for a specific threat-source,
Wdete = weight of the attack detectability for a specific threat-source,
U(x) = utility function of the attributes.

The consequences of an attack equal to the sum of the related asset attribute values, as shown in equation (3). These attributes are: the asset value, the repair cost, the reputational damage, the operational damage and the legal damage, as defined in section 3.1.

$$C(Attack) = assetValue + repaCost + repuDam + OperDam + LegalDam \ (3).$$

In order to estimate the risk of a specific threat, a risk aggregation over the constructed attack tree is required. Starting from the leafs and moving toward the root of the tree, the total risk value is aggregated according to the following:

In the OR nodes, the total risk value equals to the maximum risk value of its sub-nodes (SubN), as shown in equation (4):

$$Risk(N) = MAX(Risk(SubN_1), Risk(SubN_2), \dots, Risk(SubN_i)) \qquad (4).$$

In the AND and CAND nodes, the total risk value equals to the product of the joint probability of the sub-node events and the total consequences of the sub-node events (equation 5).

$$Risk(N) = P(SubN1 \cap SubN2 \cap \dots \cap SubNi)\ x \\ \mathrm{C}(SubN1 \cap SubN2 \cap \dots \cap SubNi) \qquad (5),$$

Where:

$$C(SubN_1 \cap SubN_2 \cap \dots \cap SubN_i) = C(SubN_1) + C(SubN_2) + \cdots + C(SubN_i) \ (6).$$

The joint probability of the sub-node events for independent attack series events equals to the product of the probabilities of each independent attack event (equation 7). On the other hand, the joint probability of the sub-node events for order-dependent attack series equals to the product of the probabilities of each attack event, in series, given the preceding events (equation 8).

$$P(SubN_1 \cap SubN_2 \cap \dots \cap SubN_i) = P(SubN_1) x\ P(SubN_2) x \dots x P(SubN_i) \ (7).$$

$$P(SubN_1 \cap SubN_2 \cap \dots \cap SubN_{\mathrm{i}}) = \\ P(SubN_1)\ x\ (SubN_2 | SubN_1) x \dots x (SubN_i | SubN_{i-1} \dots SubN_2 SubN_1) \ (8).$$

4 Risk Analysis Approach: Step-by-step

This section summarizes and presents the proposed risk analysis approach. It consists of two distinct processes: (a) risk identification and (b) risk estimation, each of which comprises a set of specific steps that are analysed bellow.

Risk Identification Process

The purpose of risk identification is twofold: (i) to determine what might happen causing potential loss, and (ii) to gain insight into how, where and why the loss occurs. To achieve this, both the business and the attacker's point-of-view should be taken into consideration. The risk identification process consists of the following five (5) steps:

Step 1: Asset Identification. In this step, anything that is important to the organization should be considered. This includes both primary assets (i.e., such as business processes/activities or information) and secondary (i.e., such as hardware, software, network, personnel, site and organization's structure). Assets' identification can be performed in various levels of details. However, the most appropriate is the one that provides sufficient information for the risk estimation process, which follows risk identification. However, since risk analysis is a recurrent procedure, the level of detail can be changed, accordingly, in further iterations of the risk analysis process.

Step 2: Threat Identification. In this step, anything that threatens assets and originates from deliberate threat-sources should be identified. These threats may arise either from inside or outside the organization. Threats should be identified as general as possible and elaborated further (i.e, going into a greater level of details), where appropriate. For every identified threat, possible threat-sources should be defined. Moreover, for each threat-source, a profile should be created giving weights to each attack attribute, using the threat-source profile matrix described in section 3.2.

Step 3: Existing Controls Identification. In this step, existing controls, if any, are identified in order to avoid unnecessary work in the next steps of the risk analysis process. According to ISO 27000, a control is the synonym of a countermeasure. Controls may reduce, minimize or even abolish the risk of a potential threat. Furthermore, in this step the efficiency of the existing controls should be verified. In many cases controls does not work as expected, creating new vulnerabilities, which should be treated either by replacing them or by implementing complementary controls.

Step 4: Vulnerability Identification. In this step, the vulnerabilities that may harm assets should be identified. Vulnerabilities may exist in an organization, processes and procedures, management routines, personnel, physical environment, information system configuration, hardware, software or even related external parties.

Step 5: Information Security Incident Identification and Identification of Corresponding Consequences. This step gets as input the identified assets, threats and vulnerabilities of the previous step and identifies the entire set of information security incidents, related to the identified threats. As mentioned above, information security incidents fall into three main categories: single attacks, independent attacks series events, and dependent attacks series events. Furthermore, the consequences that will occur by a security incident should be identified in terms of asset value, repair cost, reputational damage, operational damage and legal damage, as defined in section 3.1.

Risk Estimation Process

This process estimates, quantitatively, the risk of each threat using the tools and the mathematical formulas, described in sections 3.2 and 3.3, respectively.

Step 1: Assigning Values to Probability and Consequences Attributes. In this step specific values are assigned to each attribute related to the probability of occurrence and consequences of the identified attacks. In case of order-dependent attacks series, the attack should be examined as part of a sequence of events.

Step 2: Mapping Information Security Incidents with Threats. This step involves the construction of an attack forest. For each threat, a separate attack tree is constructed, as described in section 3.2. Extra nodes that represent intermediate system states or sub-threats should be added where necessary.

Step 3: Aggregating Risk using Attack Trees. In this step, the risk is aggregated from the leafs to the root of a tree, using the formulas described in 3.3.

5 A Simple Example

In this section, we provide a simple example where the proposed risk analysis approach is applied as a proof of concept, omitting the details of the system (such as assets, threats, vulnerabilities and attacks). After identifying the system's assets and the corresponding threats, the potential threat-source profiles should be determined. For the provided example, the following three attacker's profiles have been defined: (i) Professionals, (ii) Hackers/Crackers, and (iii) Script Kiddies (see Table 2). Using the threat-source profile matrix, weight values are assigned to each probability attribute, based on each attacker's expertise, motivation and resources.

Table 2. Threat-source Profile Matrix

	Professionals	Hackers/Crackers	Script Kiddies
Wcost	0.1	0.3	0.4
Wdetectability	0.6	0.4	0.2
Wdifficulty	0.3	0.3	0.4

It is assumed that the system under examination does not implement any security control. Moreover, it is assumed that after examining the system's vulnerabilities for a specific threat, three potential information security incidents have been identified: (1) a single attack incident, (2) an independent attacks series incident, and (3) a dependent attack series incident. Incident 1 consists of single attack A1. Incident 2 consists of attacks A2 and A3 which are two mutually independent events. Incident 3 consists of attacks A4, A5 and A6 which are three dependent events (i.e., A5 occurs under the condition that A4 have occurred and A6 occurs under the condition that both A4 and A5 have occurred). For all the attacks taking part in each identified incident, the values of attributes that are related to the probability of occurrence are assigned (see Table 3). Finally, it is assumed that the consequences of all the incidents are constant and equal to C.

Table 3. Assigned to each attack attribute values

	Incident 1	Incident 2		Incident 3		
	A1	A2	A3	A4	A5| A4	A6|A5A4
Cost	2	2	3	2	2	1
Detectability	3	1	4	2	1	1
Difficulty	4	3	1	1	1	1

Drawing the information security incidents to the single identified threat, we provide the following extended attack tree:

Theat 1
OR 1. Incident 1
    OR 1.1 Attack 1
    2. Incident 2
    AND 2.1 Attack 2
            2.2 Attack 3
    3. Incident 3
    CAND 3.1 Attack 4
            3.2 Attack 5
            3.2 Attack 6

Assuming now that we want to estimate the risk of a professional hacker realizing the threat under study. The probability of occurrence of one of the above mentioned attacks (i.e., incidents 1,2,3) by a professional hacker, according to the equation (2) and table 2, equals to:

$$P(Attack) = 0.1 \times U(cost) + 0.6 \times U(diff) + 0.3 \times U(detect)$$

By applying cost, difficulty and detectability values (see table 3) to the formula above, we get the results included in table 4:

Table 4. Attack occurrence probabilities

Incident 1	Incident 2		Incident 3		
P(A1)	P(A2)	P(A3)	P(A4)	P(A5| A4)	P(A6|A5A4)
0.30	0.55	0.70	0.65	0.95	1

Aggregating risk from the leafs to the root of the tree, using the equations (2), (7), (8), for each node of the tree, we get the following results:

$$P(Incident\ 1) = P(A1) = \ 0.30,$$
$$P(Incident\ 2) = P(A2)\ x\ P(A3) = \ 0.385,$$
$$P(Incident\ 3) = P(A4)\ x\ P(A5|A4)\ x\ PP(A6|A4A5) = \ 0.6175.$$

The risk of the root node (OR node), using the equation (4), equals to the maximum risk value of the sub-nodes, and thus:

$$\begin{aligned} Risk(Threat) = {} & MAX\big(Risk(Incident\ 1), Risk(Incident\ 2), Risk(Incident\ 3)\big) \\ = {} & MAX(0.30\ x\ C, 0.385\ x\ C, 0.385\ x\ C) = \ 0.6175\ x\ C \end{aligned}$$

6 Conclusions & Future Work

In this work, a quantitative risk analysis approach for deliberate threats is proposed and analyzed. The conceptual and mathematical foundations of the approach, as well as the tools that facilitate the process of risk estimation are elaborated. The entities and attributes that take part in the risk analysis are defined and represented, graphically, using UML class diagrams. Moreover, the tool of threat-source profile matrix is introduced in order to get insights into who and how is more likely to attack to the system under examination. The specific steps of the proposed approach are defined and analyzed, in details, and all the necessary mathematical functions are explained. Finally, a simple example of the proposed approach is presented as a proof of concept.

This work sets the scene for a full quantitative risk analysis approach for deliberate threats. In contrast to the existing methods/approaches, it is fully ISO 27005 compatible and provides a suitable level of details for deliberate threats, taking into account both the attacker and business perspectives. It provides guidance into what should be measured and how should be used in order to estimate the risk of the identified threats, but it does not provide a way how to make these measurements. Although attributes such as the cost of an attack might be easy to be measured, attributes such as the difficulty of an attack or the reputational damage can be proved highly subjective. In future work, we plan to identify ways to measure all or part of these attributes independently of the analysts' subjectivity (i.e., different analysts will be able to reproduce the same results). Furthermore, it is planned to implement the proposed approach in a real system.

References

1. Shneier, B.: Attack Trees: Modeling security threats. Dr. Dobb's Journal, http://www.schneier.com/paper-attacktrees-ddj-ft.html, (1999)
2. Shneier, B.: Secrets & Lies: Digital Security in a Networked World. John Wiley & Sons, (2000)
3. International Organization for Standarization, ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management systems – Requirements, (2005)
4. International Organization for Standarization, ISO/IEC 27002, Information technology -- Security techniques -- Code of practice for information security management, (2005)
5. International Organization for Standardization (ISO), ISO/IEC 27005: Information technology – Security techniques – Information security risk management. (2008)
6. Stoneburner, G., Goguen, A., Feringa A.: Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, NIST, (2002).
7. Computer Emergency Response Team (CERT), Carnegie Mellon University, Cert Statistics (Historical), http://www.cert.org/stats/
8. Moore, P.A., Ellison, J.R., Linger, C.R.: Attack Modeling for Information Security and Survivability, Carnegie Mellon University, Technical Note, (2001)
9. International Organization for Standarization, ISO/IEC 27000, Information technology - Security techniques - Information security management systems - Overview and vocabulary, (2009)
10. CRAMM User Guide, Version 5.0 & 5.1, http://www.cramm.com/, (2005)
11. Zaobin, G., Jiufei T., Ping W., Vijay V.: A Novel Security Risk Evaluation for Information Systems, Proceedings of the 2007 Japan-China Joint Workshop on Frontier of Computer Science and Technology, pp 67-73, (2007)
12. Benini, M., Sicari, S.: Assessing the risk to intercept VoIP calls, Journal of Computer Networks, vol 52, issue 12, pp. 2432-2446, (2008)
13. Object Management Group (OMG), Unified Modeling Language Specifications, http://www.omg.org/technology/documents/modeling_spec_catalog.htm#UML