Perceived Risk Assessment

Yudistira Asnar
Dept. of Information Science and Engineering
University of Trento
Trento, Italy
yudis.asnar@disi.unitn.it

Nicola Zannone
Department of Computer Science
University of Toronto
Toronto, Canada
zannone@cs.toronto.edu

ABSTRACT

In the last years, IT systems play a more and more fundamental role in human activities and, in particular, in critical activities such as the management of Air Traffic Control and Nuclear Power Plant. This has spurred several researchers to develop models, metrics, and methodologies for analyzing and measuring the security and dependability of critical systems. Their objective is to understand whether the risks affecting the system are acceptable or not. If risks are too high, analysts need to identify the treatments adequate to mitigate them. Existing proposals however fail to consider risks within multi-actors settings. Here, different actors participating to the system might have a different perception of risk and react consequently. In this paper, we introduce the concept of perceived risk and discuss its differences with actual risk. We also investigate the concepts necessary to capture and analyze perceived risk.

Categories and Subject Descriptors

D.2.8 [**Software Engineering**]: Metrics; D.2.1 [**Software Engineering**]: Requirements/Specifications—*languages*; K.4.3 [**Computer and Society**]: Organizational Impacts—*Reengineering*

General Terms

Security, Reliability, Measurement

Keywords

Perceived Risk, Risk Assessment, Subjective Input

1. INTRODUCTION

Nowadays, security is becoming a primary need for IT systems. Many efforts have been made toward the definition of approaches for designing secure systems in security-driven research and practices. Such efforts resulted in a number of standards (e.g., ISO 27000 series), regulations (e.g., Sarbanes-Oxley, Basel II, HIPAA), security techniques (e.g., [5, 28]), security engineering methodologies (e.g., [6, 16, 25]), metrics (e.g., [22]) and risk management frameworks (e.g., [4, 7, 12, 13, 14]).

Most of above proposals are intended to remove flaws from the system, which can be used later by attackers to compromise it. However, only few of them (i.e., security metrics and risk management frameworks) address the problem of measuring the level of security/protection of an IT system. In particular, risk management attempts to assess the expected loss (i.e., actual risk) in terms of the likelihood of events and their severity over the system.

The evidence, such as Risks-Digest [30], Common Vulnerabilities and Exposures [1] and CERT Statistic [10], suggests that many security incidents are not IT-related. For instance, users disclose personal data while using public terminals or do not change the password regularly. In this setting, risks should be analyzed within the socio-technical context, where human and organization factors, besides technical aspects, assume a critical role in the correct operation of IT systems. Those incidents are due to the perception of risk that users may have. Schneier observes that people *"overreact to intentional actions, and under-react to accidents, abstract events, and natural phenomena"* [31]. Decisions made by users can be also affected by the difficulty in quantifying the risks [22].

In this paper, we look at the problem of risk assessment from a broader perspective, accounting for organizational and social issues. In particular, we discuss the motivations behind perceived risk assessment and subjective risk assessment. We also discuss the differences between actual and perceived risk, and analyze the concepts necessary to capture and assess perceived risk.

The paper is organized as follows. Next, we present perceived risk assessment and subjective risk assessment (§2). Then, we discuss the difference between actual risk and perceived risk (§3) and investigate the concepts necessary to assess perceived risk (§4). Finally, we summarize our findings and discuss future work (§5).

2. RISK AS A SECURITY METRIC

One of the most prominent definitions of risk is proposed in [18]: risk is the *"combination of the probability of an event and its consequence [...] when there is at least the possibility of negative consequences"*. Risk thus measures the security of a system in terms of expected loss resulted from a security incident [15]. Determining the value of risks allows analysts to prioritize events and allocate the resources for safeguards with respect to their criticality.

This definition has driven the development of a number of frameworks and guidelines for risk assessment. For instance, COBIT [17], ISO 13335 [19], and ISMS [20] prescribe how to identify the threats obstructing the organization objectives, and how the organization should treat them and communicate the residual risk. CORAS [12] provides an integrated system development and risk management process for critical security systems. DDP [14] specifies how to compute the level of objectives achievement and the cost of mitigation from a set of given mitigation. The Tropos Goal-

QoP'08, October 27, 2008, Alexandria, Virginia, USA.

Risk framework [4] provides a modeling and a formal framework for assessing and treating risks within organizational settings.

However, several critics were leveled against the "well-established" risk management [11, 12, 17] as a means for the evaluation of the system security. For instance, Jaquith [22] argues that quantifying risk is a hard task since the measurement is affected by subjectivity and ignorance; these can introduce mislead evidence that influences the decision-making process. Moreover, some scholars prove that people reaction does not always reflect the actual risk [26, 31]. For instance, many studies show that people perceive driving safer than flying [31]. Conversely, the facts show that car crashes cause 42.642 deaths every year only in US; this is equivalent to have a full-load Boeing 727 crashing every 1.5 day (or 225 crashes in a year) [38]. However, according to NTSB report [39] the annual acident-rate of aviation, from 1988 - 2007, is never beyond 0.7 accident per million hours of flight (at 1989).

Our objective is to address the issues mentioned above: *perceived risk assessment* and *subjective risk assessment*. Perceived risk assessment attempts to understand the actor perception of a particular risk [9]. In particular, we want to devise a framework for assessing risks in the context of socio-technical systems that considers not only expected loss, but also the risks perceived by the different users within the system.

Subjective risk assessment is intended to asses risks when there is a lack of objective data (e.g., statistic from past experience, empirical experiments). This lack is also due to the several "black-swan" events that have a hardly predictable impact, and rare events beyond the current knowledge, which characterize IT-security. For instance, administrators used to assume that, if the access to Internet is only through an HTTP-proxy, the users cannot make voice communications. However, it is not the case anymore because several VoIP protocols (e.g., Skype, GTalk-XMPP) are not blocked by the proxy. Some studies [33, 41] have shown that the Dempster-Shaffer theory of evidence [34] is more appropriate to support subjective risk assessment than the Kolmogorov Probability theory.

- The Kolmogorov Probability theory assumes that the probability that an event A does not occur ($P(\neg A)$) can be inferred from $P(A)$

$$P(\neg A) = 1 - P(A)$$

- The Dempster-Shaffer theory allows us to capture the notion of "ignorance" (X).[1] Accordingly, the evidence that A does not occur ($E(\neg A)$) cannot be inferred from the evidence of $E(A)$

$$E(\neg A) \leq 1 - E(A)$$

  and ignorance cannot infer neither A nor $\neg A$.

The challenge for the subjective risk assessment is thus to provide analysts with a "good enough" decision-making support using subjective data.

In summary, methods for risk assessment can be classified with respect to two dimensions: perception and input. Table 1 provides a taxonomy of existing methods. In actual risk assessment, we find proposals that consider both objective and subjective inputs. For instance, Probabilistic Risk Analysis (PRA) [7] or Fault Tree Analysis (FTA) [37] assess the risk of system using inputs gathered from experiments or empirical data, whereas Bayesian [29] and Belief-based [23] use inputs from experts' judgment. On the contrary, we have not found effective methods for perceived risk assessment in the literature. Working towards this direction, we notice that analysts need to consider actors' mental-states (e.g., expectation, risk behavior), that are subjective data. Accordingly, our work can be classified as a method for assessing perceived risk using subjective data (Table 1).

Input / Perspective	Objective	Subjective
Actual	PRA [7], FTA [37], DDP [14], CORAS [12]	Bayesian [29], Belief-based [23], Goal-Risk [4]
Perceive	N/A	our research direction

Table 1: Risk Assessment Methods

In this paper we mainly focus on the perspective dimension and the concepts necessary to capture and analyze it. We also discuss the differences between actual and perceived risk. Details on subjective risk assessment can be found in [2].

3. ACTUAL RISK VS PERCEIVED RISK

Risk is the expected loss due to a negative event. Based on that value, users make decisions that attempt to minimize risks. However, some studies [26, 31] demonstrate that on many occasions users behave otherwise. For instance, people perceive driving safer than flying though it is shown statistically otherwise.

Those studies call for a distinction between risk and the perception of it. Essentially, users behave according to their perception of risk rather than to the actual risk. Several aspects can influence user perception, such as trust towards other actors, social norms, and risk/event characteristics (e.g., intentionality, recency, spectacularity) [31, 35]; also the way in which risks are communicated can affect the user perception [27].

The trust of users towards other users or towards the system is surely a fundamental aspect for assessing perceived risk. Lacoheea et al. [26] show that there are strong relations among security, risk, and trust in affecting the behaviors of Internet users (i.e., decision to buy via online). In particular, trust affects the user perception of risk. For instance, if a user trusts the system administrator and the administrator suggests him to adopt a safeguard to reduce risks, the user expects that such a safeguard effectively reduce the risks. Conversely, if a manager distrusts one of his subordinates to perform a critical task, he feels that appointing that subordinate to perform the task is at high risk.

The perception of risk is closely related with user expectations and preferences. User expectations represent the user feeling that something is about to happen, and user preferences capture the predisposition in favor of something. Different users can have different expectations for the same situation. Perceived risk can be seen as the distance between user expectations and preferences and the risks that users tolerate. For instance, if the expected loss of two events are the same but a user tolerates a risk more than the other, the user perceives one event more risky than the other. Expectations also include the opportunities that users have when taking a risk. A concrete example is given by the number of people gambling.

Moreover, perceived risk is also related with culture and norms of a particular society [31]. For instance, Indonesian citizens argue that e-Commerce is extremely risky, while EU citizens have a different perception of it. In any case, when a user is on the Internet, he is exposed to the same set of hackers. The different perception of risk between Indonesian and EU citizens is caused by the fact that e-Commerce transactions are not a common means in the In-

[1] *Ignorance* refers to the uncertain situation where either event A occurs or not. Mathematically, it is written as $E([A, \neg A])$.

donesian society. This aspect of perceived risk might also explain why driving is not perceived as dangerous: driving is considered an ordinary activity in almost every society.

Risk management aims to reduce the likelihood of events or their impacts within an acceptable level. This approach however is not suitable to manage perceived risk; users might behave carelessly because they know that they are exposed to risks remotely or because they seek opportunities. The aim of perceived risk management is to correct the user perception, advising users when their perception diverges from actual risk.

4. PERCEIVED RISK CONCEPTS

From the previous section, it is evident that perceived risk is related to user believes (e.g., culture and norms) and expectations (e.g., opportunities). Perceived risk assessment demands the definition of a conceptual model that allows analysts to capture those aspects besides including the concepts necessary to assess actual risk and to analyze organizations. In this paper, we investigate three concepts specific to perceived risks: utility, risk tolerance, and trust.

Utility is the value generated by assets.[2] The loss can be seen as the reduction of utility [4]. Some approaches quantify the loss on the basis of the asset value (e.g., price of a web server) [12] or of actuary/analyst judgment [40]. Conceptually, the notions of utility and value are different [8]: the utility of an asset is assessed by summing up all the values generated by the asset. For instance, an on-line book store can have web servers for a value of 10K Euro, but they generates utility much more beyond that value. Every user might also specify a different utility for the same asset. For instance, the book store payment clearing system has more utility for the sales division than for the finance division. As consequence, a user can perceive an expected loss different from the loss expected by another user for the same event. Specifying the loss as a value function or analysts judgment does not make it possible to capture such issues, because the price/value of an asset is independent from which actors are assessing it.

Risk tolerance is the expected (utility) loss acceptable by users. As mentioned before, perceived risk is not an absolute value; it can be defined as the distance between the risk tolerance and expected loss. For instance, two users – Alice and Bob – expose to the risk of loosing 2K on a transaction. The income of the two users is different, let say, Alice earns 100K/year and Bob 50K/year. In this setting, Bob can argue that the transaction is risky, while Alice is more willing to accept the risk. Risk tolerance can be used to represent user expectations and preferences.

Trust captures a user's (the trustor) belief that another user (the trustee) behaves according to an agreement (the trustum). Trust is characterized by a level which represents the degree of trust between two users. Many researchers have investigated the relationships between trust and risk. Jøsang and Lo Presti [24] notice that trust and risk drive the decision-making process. Risk is used as a measure of reliability trust (i.e., the probability of having a successful transaction); reliability trust together with the risk attitude of a user supports the user in making (trust) decisions. Solhaug et al. [36] emphasize that risk cannot be inferred from trust because trust does not include aspects concerning the impact in case the trustee betrays. Asnar et al. [3] underline the fact that users expose to risks because they depend on other users for accomplish some task and not because of trust. In other words, there is no harm in trusting someone. These proposals however, attempt to assess actual risk. For instance, if Bob depends on Alice for some tasks, the actual risk is the same whether or not Bob trusts Alice. What changes is Bob's perception of risk: if Bob trusts Alice, he believes that Alice carries out the task. In this work, we have identified two types of trust relevant to perceived risk: trust in execution and trust in evidence. *Trust in execution* represents the trustor belief of the capability and dependability of the trustee in fulfilling the trustum. *Trust in evidence* represents the trustor belief of the evidence provided by the trustee about the trustum. For instance, if Bob trusts (in execution) the book store for handling books, he perceives that the store handles books properly. In this setting, the perceived risk is deduced independently from the risks suffered by the book store. Conversely, if Alice trusts (in evidence) the book store for handling books, her perception of risk depends on the risks suffered by the store. In case the book store discloses a report stating that the fraud rate is increased, Alice's perceived risk increases, while Bob's perceived risk does not change.[3]

5. OUR VISION

The risk attitude of users is driven by their perception of risk [31, 26]. Weber et al. [42] propose a more sophisticated model defining the risk attitude of an actor by consider also expected benefit over the risks and the user risk behavior (e.g., risk seeker, risk neutral, and risk aversion). New models of risk attitude are demanded as all proposed models do not consider the user rationale (i.e., goals, preferences) and trust.

Many systems are operated in a socio-technical context where humans play a critical role in maintaining system security. Besides advising users when their perception diverges from actual risk, the perceive risk model can be used to tune the risk perception at the "correct" level. Conventionally, risk management intends to suppress the risk level as much as possible (e.g., the cost is still lower then the benefit). This however does not apply to perceived risk because a low perception of risk can lead users to behave carelessly, whereas a high perception results in user stress. We believe that criteria of "correct" are grounded in the application domain. Essentially, there are three basic settings of "correct":

1. keep perceived risk equal then the actual one,
2. keep perceive risk lower then the actual one,
3. keep perceive risk higher ten the actual one.

In a bank system, security controls should mitigate risks as much as possible, but leave the impression that the system is still at risk to keep users prudent This situation fits in the third case. Conversely, in Air Traffic Management, a high perceived risk makes controllers working under pressure. Consequently, the controllers are prone to errors that compromise the security and safety of the system. Thus, the most appropriate setting is the second one, but the difference between actual and perceived risk should not be too high because it can lead the controllers to behave careless. The decisions about the setting to be adopted and the divergence between actual and

[2] Adam Smith defines the value of goods into two classes: value-in-exchange and value-in-production. In this paper, we call the former as "value" and the later as "utility"

[3] We assume that the book store report does not modify Bob's trust toward it.

perceived risk should be made carefully and take into account the sustainability of the organization in the long run.

In addition, the understanding of how different aspects affect risk perception is still challenging. For example, even if user expectations and preferences rule the risk tolerance, users are more sensitive for their expectations than for their preferences [31]. As consequences, users are more inclined to over-react to risks that obstruct their expectations than to risks that obstruct their preferences.

Once the perceive risks is assessed, analysts needs support to treat/manage assessed risks. Surely, all types of risk treatments [21] (e.g., reduction, retention, avoidance, transfer), that are applicable for mitigating actual risks, are useful also to manage the risk perception. In addition, there are other means such risk communication [21], security theater [32], that may not mitigate the actual risk, but affect the risk perception. Risk communication intends to let actors understand the risks that threaten them. At the end, the risk perception of actors can be higher/lower then before depending on the level of actual risk (i.e., it reduces the difference between perception and actual risk. Security theater is a term for security controls that give an impression that they mitigate the risks though in reality they do not mitigate either the likelihood nor the severity.

Risk management usually analyzes risks from the perspective of the "owner" of the system (e.g., CEO, president, shareholders). Perceived risk management extends this vision by considering every user within the system and the relations among users. In this setting, it is also possible to analyze events that are perceived as risks by some users and as opportunities by other users.

Future work includes the definition of a framework for assessing both actual and perceived risks within an organization that supports subjective and objective inputs. This is only the first step as we want to assess the system quality with respect to risk.

Acknowledgments

This work has been partially funded by the EU SERENITY and MASTER projects, and by the Canada's NSERC Hyperion project. We thank to Fabio Massacci and Paolo Giorgini for useful comments and discussions.

6. REFERENCES

[1] CVE - Common Vulnerabilities and Exposures. http://cve.mitre.org/. accessed at 2008-05-27.

[2] Y. Asnar and P. Giorgini. Analysing Risk-Countermeasure in Organizations: a Quantitative Approach. Technical Report DIT-07-047, DIT - University of Trento, July 2007.

[3] Y. Asnar, P. Giorgini, F. Massacci, and N. Zannone. From Trust to Dependability through Risk Analysis. In *Proceedings of the Second International Conference on Availability, Reliability and Security*. IEEE Press, 2007.

[4] Y. Asnar, R. Moretti, M. Sebastianis, and N. Zannone. Risk as Dependability Metrics for the Evaluation of Business Solutions: A Model-driven Approach. In *Proceedings of the 3rd International Workshop on Dependability Aspects on Data WArehousing and Mining applications*, 2008.

[5] R. G. Bace. *Intrusion Detection*. Sams Publishing, 2000.

[6] D. Basin, J. Doser, and T. Lodderstedt. Model Driven Security: From UML Models to Access Control Infrastructures. *ACM Transactions on Software Engineering and Methodology*, 15:39–91, 2006.

[7] T. Bedford and R. Cooke. *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, 2001.

[8] D. Bernoulli. Exposition of a New Theory on the Measurement of Risk. *Econometrica*, 22:23–36, 1954. (original 1738).

[9] J. R. Bettman. Perceived risk and its components: A model and empirical test. *Journal of Marketing Research*, 10:184–190, 1973.

[10] CERT. Cert statistics. http://www.cert.org/stats/. accessed at 2008-05-27.

[11] COSO. *Enterprise Risk Management - Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission, September 2004.

[12] F. den Braber, T. Dimitrakos, B. A. Gran, M. S. Lund, K. Stølen, and J. Ø. Aagedal. The CORAS Methodology: Model-Based Risk Assessment using UML and UP. In *UML and the Unified Process*, pages 332–357. Idea Group Publishing, 2003.

[13] DoD. Military Standard, Procedures for Performing a Failure Mode, Effects, and Critical Analysis. MIL-STD-1629A, 1980.

[14] M. S. Feather. Towards a Unified Approach to the Representation of, and Reasoning with, Probabilistic Risk Information about Software and its System Interface. In *Proceedings of the 15th IEEE International Symposium on Software Software Reliability Engineering*, pages 391–402. IEEE Computer Society Press, November 2004.

[15] D. Geer. Risk Management is Still Where the Money is. *Computer*, 36:129–131, 2003.

[16] P. Giorgini, F. Massacci, J. Mylopoulos, and N. Zannone. Modeling Security Requirements Through Ownership, Permission and Delegation. In *Proceedings of the 13th IEEE International Requirements Engineering Conference*, pages 167–176. IEEE Computer Society Press, 2005.

[17] T. I. G. Institute. *CoBIT - Framework Control Objectives Management Guidelines Maturity Models*, 4.1 edition.

[18] ISO/IEC. Risk Management-Vocabulary-Guidelines for Use in Standards. ISO/IEC Guide 73, 2002.

[19] ISO/IEC. Management of Information and Communication Technology Security - Part 1: Concepts and Models for Information and Communication Technology Security Management. ISO/IEC 13335, 2004.

[20] ISO/IEC. Information Technology - Security Techniques - Information Security Management Systems - Requirements. ISO/IEC 27001, 2005.

[21] ISO/IEC. Information Technology - Security Techniques - Information Security Risk Management. ISO/IEC 27005, 2008.

[22] A. Jaquith. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison Wesley, 2007.

[23] A. Jøsang, D. Bradley, and S. J. Knapskog. Belief-Based Risk Analysis. In *Proceedings of the 2nd Workshop on Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation*, pages 63–68, Darlinghurst, Australia, Australia, 2004. Australian Computer Society, Inc.

[24] A. Jøsang and S. Presti. Analysing the Relationship Between Risk and Trust. In *Proceedings of the Second International Conference on Trust Management*, volume 2995 of *Lecture Notes in Computer Science*, pages 135–145. Springer-Verlag, 2004.

[25] J. Jürjens. *Secure Systems Development With UML*. Springer, 2005.

[26] H. Lacoheea, A. Phippenb, and S. Furnell. Risk and Restitution: Assessing How Users Establish Online Trust. *Computers & Security*, 25(7):286–293, October 2006.

[27] D. G. Mayo and R. D. Hollander. *Acceptable Evidence: Science and Values in Risk Management*. Oxford University Press US, 1991.

[28] G. McGraw. *Software Security: Building Security in*. Addison-Wesley, 2006.

[29] A. Mosleh, E. R. Hilton, and P. S. Browne. Bayesian probabilistic risk analysis. *SIGMETRICS Perform. Eval. Rev.*, 13(1):5–12, 1985.

[30] P. G. Neumann. RISKS-LIST: RISKS-FORUM Digest. http://catless.ncl.ac.uk/Risks/. accessed at 2008-05-27.

[31] B. Schneier. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Springer, 2003.

[32] B. Schneier. In Praise of Security Theater. http://www.schneier.com/blog/, January 2007. last access 04.08.2008.

[33] K. Sentz and S. Ferson. Combination of Evidence in Dempster-Shafer Theory. Technical Report SAND 2002-0835, Sandia National Laboratories, 2002.

[34] G. Shafer. *A Mathematical Theory of Evidence*. Princeton University Press, Princeton, NJ, 1976.

[35] P. Slovic. Perceived Risk, Trust, and Democracy. *Risk Analysis*, 13(6):675–682, 1993.

[36] B. Solhaug, D. Elgesem, and K. Stølen. Why Trust is not Proportional to Risk. In *Proceedings of the Second International Conference on Availability, Reliability and Security*. IEEE Press, 2007.

[37] M. Stamatelatos, W. Vesely, J. Dugan, J. Fragola, J. Minarick, and J. Railsback. *Fault Tree Handbook with Aerospace Applications*. NASA, 2002.

[38] U.S. NCSA - NHTSA. Fatality Analysis Reporting System General Estimates System - 2006 Data Summary. http://www-nrd.nhtsa.dot.gov/CMSWeb/, 2008. last access 04.08.2008.

[39] U.S. NTSB. Aviation Accident Statistics. http://www.ntsb.gov/aviation/Table2.htm, 2008. last access 04.08.2008.

[40] D. Vose. *Risk Analysis: A Quantitative Guide*. Wiley, 2000.

[41] P. P. Wakker. Dempster Belief Functions are based on the Principle of Complete Ignorance. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 8(3):271–284, 2000.

[42] E. Weber, A. Blais, and N. Betz. A Domain-Specific Risk-Attitude Scale: Measuring Risk Perceptions and Risk Behaviors. *Journal of Behavioral Decision Making*, 15(4):263–290, 2002.