A Cause and Effect Approach Towards Risk Analysis

Laleh Pirzadeh
Department of Computer Science and Engineering
Chalmers University of Technology
Göteborg, Sweden
laleh.pirzadeh@chalmers.se

Erland Jonsson
Department of Computer Science as Engineering
Chalmers University of Technology
Göteborg, Sweden
erland.jonsson@chalmers.se

***Abstract*— Risk analysis is critical for IT systems and for organizations and their daily operation. There are various tools and methods to analyse risk. Most approaches take risk assessment as a result of specific factors (such as threats and vulnerabilities) without investigating the impact of various types of system operation. Therefore, we suggest a causal approach toward risk analysis based on an existing security model. We start out from a current risk analysis method and improve it by taking the system operation, causal relation between the impairments, as well as latency effects into account. The approach exhibits the impact of the attack chain of impairments on system risk. We claim that the approach presented in this paper will make it possible to conduct a more refined quantitative assessment of risk.**

Keywords- security model; risk analysis; causal chain of impairments; metrics; security planning; system operation

I. INTRODUCTION

Most IT organizations need to deal with different types of daily decision making such as budget planning and security investment choices. Risk analysis is a critical task performed by CIOs and managers enhancing the decision making process. Although formal risk analysis is required by ANSI 2008 (for IT systems) and Basel II (Financial regulations for Operational Risk), it is not necessarily part of the current security management of many IT organizations.

Due to the criticality of a precise method for assessing risk while making decisions, we suggest a novel approach toward risk analysis based on the causal chain of impairments. See section III.B. This approach is founded upon a previously proposed security model [10], where security is quantified according to its interaction with the environment. The model can be applied to risk analysis so as to incorporate influence from internal system operations.

There have been various proposals for risk calculations within organizations and industry. These methods vary from qualitative to quantitative risk analysis. Qualitative approaches are useful for more abstract levels of analysis and comparison. However, risk quantification methods such as Reduced Risk [5], [25] and Risk based Return on Investments (RROI) [7] take us one step further and offer more refined information on system risk by identifying the gained benefit or reduced risks.

Current approaches for risk analysis and quantification are in many cases based on a very simplistic assumption about the relation between risk event and risk impact. What is missing in these methods is the probabilistic influence from the system operation, internal mechanisms and the impairments on system risk. Indeed, other authors have suggested more refined risk analysis methods, such as the probabilistic distribution among successful attacks [23] or calculating the effect of aggregating different tasks in a complex business process [24]. However, none of them has adopted the full input-output causal approach as the one presented in this paper.

Thus, we suggest that risk analysis should incorporate the influence of the propagation of impairments, system operation and latency on the system behaviour (output). This means that for a single attack (input) all possible outcomes (outputs) are calculated with their respective probability and delay, so as to add up to a composite risk assessment.

In the following, section II gives a brief summary of the current research state in risk analysis. The security model and its chain of impairments are described in section III. In section IV the implications of the model to risk analysis is discussed. The paper is concluded in section V.

II. CURRENT STATE IN RISK ANALSYSIS RESEARCH

There have been quite a number of approaches toward risk assessment and analysis. We will not try to cover all the existing approaches and tools but rather give a brief review over some representative methodologies. In this paper we adopt the definition by Ralston et al. [5] where risk assessment is defined as a multiphase process consisting of Risk Identification, Risk Analysis, Risk Evaluation and Ranking, and Management and Treatment phases. Risk assessment can be categorized into two main categories i.e. qualitative and quantitative. One general issue that should be noted for both groups is the necessity of identifying resources to be protected (targets), the threats in the environment, and vulnerabilities existing within the systems. A novel qualitative security risk assessment approach based on vulnerability analysis has been proposed by Elahi et al. [20] which is applicable in early requirement engineering phase. A list of existing risk assessment tools is provided by the Riskworld website [22] among which OCTAVE [27], RISKWATCH [28] and CORAS [26] are common.

Quantitative risk analysis methods are subcategories of Probabilistic Risk Assessment methods (PRA) [5] where the risk associated with complex technological entities is analyzed by assuming to have the knowledge about different risks in the system. Different scenarios,

frequencies, and their consequences in terms of impact are presented in PRA. In this approach, the risk metric is a consequence-oriented figure of merit, e.g. the probability of the top event [5]. However, determining the basic event probabilities is the most challenging phase in this approach. See [2], [4] for more details on PRA. Some of the popular PRA methods are Fault/Attack Tree Analysis [1-3], Event Tree Analysis [2], Failure Mode and Effect Analysis [15], [16], Failure Mode Effect and Criticality Analysis [17], [18], Cause/Consequence Analysis, Directed graphs and logical diagrams methods [4] and MORDA [21].

Another approach for risk assessment is the cost-benefit risk assessment model proposed by Wyss et al. [8]. In this approach the decision makers are capable to perform risk-based cost-benefit prioritization of various security investments/mechanisms. Their risk metric is based on the degree of difficulty for a successful attack (effort-based approach).

One of the most commonly used quantitative risk models is RROI (Risk based Return On Investment) [7] which calculates risk based on net bypass rate, incident risk, baseline scenario, and net benefit as shown in equation (1).

$$RROI = \frac{Baseline\ Scenario - Residual\ risk - Cost}{Cost} \quad (1)$$

Return On Security Investment [6] is a similar approach based on ROI and calculates risk as shown in equation (2). This approach incorporates risk exposure and percentage of risk mitigated for different security mechanisms when calculating ROSI therefore enhancing comparison between these mechanisms.

$$ROSI = \frac{(Risk\ Exposure * \%Risk\ Mitigrated) - Solution\ Cost}{Solution\ Cost} \quad (2)$$

Influence and Decisions Diagrams [13], is a decision driven approach toward risk analysis that calculates risk based on utility functions and net benefits.

A model-based approach for quantitative enterprise security assessment (Quality of Protection) was provided by [23]. In this model the number of attacks from certain threats is measured and their relative likelihood of propagation among the "dependencies" in the underlying enterprise model is estimated. This approach is based on a "Security Meta Model" and "Threat Graph", which is relatively similar to the attack tree concept. The Security Meta Model defines risk as "any threat that targets a specific model element and may result in the violation of a security requirement".

Quantified risk is another proposed method for the decision-making process in security [15]. This method is based on the probabilities and losses of events. Thus, prospect theory, rationality, reframing and normative frameworks have been discussed in detail.

U.S. Department of Homeland Security proposed the following equation (3) to calculate risk based on vulnerabilities, threats, and their impact [9].

$$RISK = Threat * Vulnerability * Impact \quad (3)$$

Where:

- ***Threat*** denotes the expected number of attacks of a particular type within a specified time unit
- ***Vulnerability*** is the extent to which the organization or system is vulnerable to the threat and gets affected, and
- ***Impact*** is the costs of the harm as loss in terms of monetary/reputation/market loss.

This approach is useful for calculating risk for different IT systems in hostile environments.

The most common formula for calculating risk is presented in equation (4).

$$RISK = Likelihood * Loss \quad (4)$$

This approach is the basis of our proposal in the paper. The risk of a bad event exposure is calculated according to the loss (consequences) and its probability/likelihood of occurrence (frequency). We discuss more about this method in section IV.

III. SECURITY MODEL AND CHAIN OF IMPAIRMENTS

In this section we explain the security model, which is the basis for our proposal on model based risk analysis. Furthermore we discuss the causal chain of impairments and its role in risk analysis.

A. The security model

Previously we have introduced an integrated security and dependability model based on the system's interaction with its environment [10]. The basic idea behind this model is to analyse system security in relation to its environment, in terms of system input and output thus enhancing the cause and effect concept.

The model proposes three categories of security attributes: protective, correctness, and behavioural. The protective attribute is integrity, which identifies a system's capability of preventing fault introduction. The output from the system is considered as the system behaviour. The behaviour must be different for authorized users and unauthorized users. Thus, the requirement on the system is that it must deliver its information (or service) to authorized users. This is the availability attribute. However, it must not deliver information to unauthorized users, as reflected by the confidentiality requirement. Other behavioural attributes are reliability and safety. See [10], [11] for more details.

B. Chain of Impairments

One of the advantages of our security model is its clear exhibition of the causal chain of impairments, from threat and attack to the system failure, see Figure 1. This (cause and effect concept) is the basis of our

proposed approach toward risk analysis. Here we give an explanation of the causal chain of impairments.

An attack is launched by a threat from the system's input environment. If successful in bypassing the boundary protection mechanisms (if any) there is an intrusion, which puts the system in an unwanted state. This system state is called an internal system error. Depending on recovery mechanisms and system operations there are three possible outcomes of this situation. The first case is when some internal recovery mechanism is able to remove the error. Thus, no failure (behavioural failure) will occur. A second case is when the error becomes latent in the system until it propagates to the output thus causing a failure after some delay, which may be short or long. The latency time varies based on the attacker intention, system operation, and error characteristics. See [14]. Please note that a high latency, i.e. a long delay before the output is influenced, is equivalent to better system behaviour, e.g. higher reliability, and thus reduced risk. In the limit, i.e. for an infinite latency, there will be no risk at all. The final case happens when the system failure occurs without noticeable delay, as a result of negligible error latency.

Thus, we see how an attack may cause an error that propagates to cause a failure. This highlights the relation between integrity on one side and behavioural attributes such as reliability, availability, safety and confidentiality on the other. The relation between the attacks and the service is a complicated issue that calls for further investigation of internal system factors and the attack characteristics.

However, there are other causes for system failure other than malicious attacks. Another such case is when a failure occurs without any external threat or attack, e.g. due to the breakdown of a physical component. Figure 1 illustrates the main phases of the causal chain of impairments of the attack process.

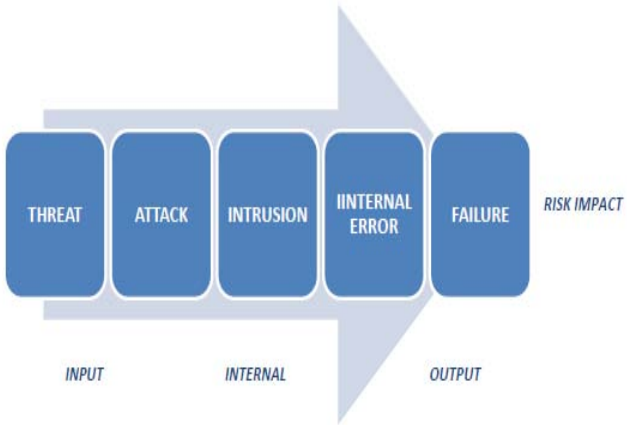

Figure 1. Chain of Impairments and Risk

IV. IMLICATIONS OF THE SECURITY MODEL FOR RISK ANALYSIS

In this section we show how the security model could be used for making a refined and more detailed risk analysis that would also incorporate influence from the system's internal operation.

A. *Rationale*

Risk is basically an interpretation of the event occurrence probability by assessing its effects on our system. The traditional and common definition of risk analysis covers the answers to the three fundamental questions [8], [19]:

1. ***What*** can happen?
2. What is ***the probability (likelihood)*** of it to happen?
3. What are the ***consequences*** and ***impact (loss)*** if something happens?

Based on these questions we formulate risk by the following equation.

$$RISK = Event * Likelihood * Loss \quad (5)$$

Where:

- ***Event*** denotes some kind of initiating detrimental influence on the system, e.g. an attack, possibly leading to a system failure,
- ***Likelihood*** denotes the probability of the Event occurrence, and
- ***Loss/Impact*** indicates the resulting consequences caused by the Event including monetary, resource or other loss

Although this approach is being applied to decision making processes by CIOs and managers, it has a major shortage. The main issue is that it has an abstract perspective and does not take the cause and effect relations between input events and output effects into account.

B. *An improved method for risk analysis*

In this section we propose an improved approach for risk analysis. This approach takes the system's operation, the internal factors and the chain of impairments into account for risk analysis, which means that we can more accurately model risk analysis than before. It is worthy to note that different types of Events can lead to similar types of failures. This is the result of the effect of varying impairment propagation and dynamic system operations. On the other hand, and for the same type of reasons, the same Event can cause different types of failures, where each type of failure comes with a specific probability. Thus, there is not a one-to-one relation between an Event and the corresponding Impact as described in equation (5). Rather, the relation is a probabilistic one-to-many, in the sense that each generating event can lead to several failures and several corresponding losses, all of them with a related probability. This can be reflected in the following improved equation for risk assessment:

$$RISK = Event * Likelihood * \Sigma\,(Probability\ of\ Propagation * Loss) \quad (6)$$

Here:

- ***Event*** denotes some kind of initiating detrimental influence on the system, e.g. an attack, possibly leading to a system failure,

- ***Likelihood (Probability of Occurrence)*** is the probability that the Event occurs,
- ***Probability of Propagation*** is the probability that an Event leads to a specific failure. This failure is one of the possible failures that may result from a specific Event,
- ***Loss*** is the loss (e.g. in EUR) associated with each failure that the Event can lead to, and
- ***Sum*** is taken over all possible failures related to one specific Event with their related losses.

Thus, equation (6) permits considering influence from system-internal factors on the risk assessment, something that is not possible when using equation (5). This is addressed by taking the sum over all different propagations of system internal operation initiated by the same Event. As mentioned in section III.B the same Event might lead to various failures. For instance in a PC depending on an antivirus program, the same threat can lead to different system failures depending on the various outcomes of the program and these will all be taken into account in the risk calculation.

V. CONCLUSION

We have proposed an improved approach to risk analysis and quantification. The approach is based on an earlier suggested security model and its causal chain of impairments. The model describes system security based on its interaction with the environment. Accordingly the proposed risk analysis method provides a clear exhibition of the system operation and attack impact on system behaviour and in particular system failure. Therefore, this approach is more fine-grained than many other risk analysis methods. However, the probabilistic relations among different system's internal operations/mechanisms and their influence on the system failure call for further investigation. As a conclusion, this approach improves risk analysis by considering more details about system operation.

REFERENCE

[1] Schneier, "Attack Trees," Dr. Dobb's Journal, December 1999, http://www.schneier.com/paper-attacktrees-ddj-ft.html, accessed March 2006.

[2] W. Vesely, M. Stamatelalos, J. Dugan, J. Fragola, J. Minarick, "Fault Tree Handbook with Aerospace Applications," Report by NASA Office of Safety and Mission Assurance, August 2002, http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf, accessed April 2006.

[3] W. Vesely, "Fault Tree Analysis (FTA): Concepts and Applications," NASA document, http://www.hq.nasa.gov/office/codeq/risk/ftacourse.pdf, accessed April 2006.

[4] E. Henley, H. Kumamoto, "Probabilistic Risk Assessment", 2nd edition, IEEE Press, New York, 1996.

[5] Dr. Patricia A. Ralston, Dr. James H. Graham and Dr. Sandip C. Patel., "Literature Review of Security and Risk Assessment of SCADA and DCS systems", Technical Report TR-ISRL-06-01, 2006

[6] W. Sonnenreich, J. Albanese, and B. Stout, "Return On Security Investment (ROSI): A Practical Quantitative Model", in Proc. WOSIS, 2005, pp.239-252.

[7] Arora, A.; Hall, D.; Piato, C.A.; Ramsey, D.; Telang, R.; "Measuring the risk-based value of IT security solutions", IT Professional , vol.6, no.6, pp. 35- 42, Nov.-Dec. 2004

[8] 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

[9] U.S. Department of Homeland Security Risk Steering Committee, "Risk Lexicon," U.S. Department of Homeland Security, Washington, DC., September 2008.

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

[11] E.Jonsson, L.Pirzadeh, "A Framework for Security Metrics Based on Operational System Attributes", Technical report, Chalmers University of Technology, 2011

[12] V.Verendel, "The Security Gap: Bias for Quantified Risk", Technical report, Chalmers University of Technology, 2010

[13] Kevin J. Soo Hoo, " How Much Is Enough?A Risk-Management Approach to Computer Security", working paper, Consortium for Research on Information Security and Policy (CRISP) June 2000

[14] E. N. Adams, "Optimizing preventive service of software products", IBM Journal of Research and Development, vol. 28, No. 1, pp. 2-14, 1984.

[15] Dependability - Analysis techniques for system reliability - Procedure for failure mode and effectsanalysis (FMEA), SS-IEC 812,2 pages, 1988

[16] Process Failure Mode and Effects Analysis (FMEA), JEP131, 19 pages, 1998

[17] Bowles, J.B.; , "The new SAE FMECA standard," Reliability and Maintainability Symposium, 1998. Proceedings., Annual , vol., no., pp.48-53, 19-22 Jan 1998

[18] "The FMECA Process in the Concurrent Engineering (CE) Environment", Society of Automotive Engineers Aerospace Information Report AIR4845, Approx. 10 co-authors, June 1993.

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

[20] G. Elahi, E. Yu, N. Zannone, "Vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities," Requirements Engineering, Special Issue on RE09, vol. 15, No.1, March 2010

[21] Buckshaw, D. L., Parnell, G.S., Unkenholz, W.L., Parks, D.L., Wallner, J.M., & Saydjari, O.S, "Mission Oriented Risk and Design Analysis of Critical Information Systems," Military Operations Research, vol. 10, No. 2, pp. 19-38, 2005.

[22] Riskworld website available at: http://www.riskworld.com/SOFTWARE/SW5SW001.HTM

[23] 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

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

[25] G. D. Tolbert, "Residual Risk Reduction," Professional Safety, pp. 25-33, November 2005

[26] CORAS website available at: http://coras.sourceforge.net/

[27] P. Marek, J. Paulina, "The OCTAVE methodology as a risk analysis tool for businessresources", In Proc. Of the International Multiconference on Computer Science and Information Technology, pp. 485-497, 2006

[28] RISKWATCH website available at: http://www.riskwatch.com/