Context-Sensitive Information Security Risk Identification and Evaluation Techniques

Dan Ionita
Services, Cybersecurity and Safety Research Group,
University of Twente,
The Netherlands
d.ionita@utwente.nl

***Abstract*—The objective of my research is to improve and support the process of Information security Risk Assessment by designing a scalable Risk argumentation framework for socio-digital-technical Risk. Due to the various types of IT systems, diversity of architectures and dynamic nature of Risk, there is no one-size-fits all RA method. As such, the research hopes to identify guidelines for conducting Risk Assessments in contexts that raise special challenges such as Telecom and virtualized infrastructures. Finally, it will suggest ways of qualitatively and quantitatively evaluating Information Security Risks in such scenarios by using argumentation and/or modelling attacker business cases.**

I. Introduction

A Risk Assessment (RA) is a structured or semi-structured approach to analysing the security of an infrastructure, identifying weak spots, and selecting countermeasures [1]. Risk Assessments can be viewed as instances of Requirements Engineering processes as they produce desired (security) properties of the target system based on higher-level (security) goals.

Currently, (Information Security) Risk Assessments are conducted mostly via brainstorming sessions where a group of experts look at an architecture[1] and try to find and rank vulnerabilities based on the estimated likelihood and impact of their exploitation, while proposing countermeasures that could mitigate the most dangerous of these so as to reach an acceptable level of risk.

The work will be undertaken as part of the TREsPASS [2] Information Security project. The project aims to improve the way companies secure information by integrating the digital, technical and social domains with the current state-of-the-art in the field of security. One of the main goals of the project is to develop an alternative Risk Assessment methodology, built around a so-called "Attack Navigator" that can predict, prioritise and prevent common risks as well as new and complex attacks. This should provide companies with an extensive, tool-supported, automated way of conducting systematic Risk Assessments. The research described in this paper is conducted in the context of the TREsPASS project, which in turn is financed by the EU.

The project aims at being applicable to a large variety of systems, ranging from Cloud to Telecom. As such, my task is to find out (1) which classes of targets of assessments exist and (2) which architectural views and argumentation techniques are most suitable for each one. The second goal stems from my hypothesis that, in some contexts, argumentation could compensate for the fact that probabilities and impacts are often not quantitatively known. Constructing arguments often requires referring to structural (architectural) properties of the Target of Assessment and its context. These properties can be represented using architectural views such as a communication diagram. Another useful view for arguing about certain kinds of risk could be the network business model. As such, I will also investigate the applicability of business modelling languages in defining attacker business cases and identifying and describing attacks. Finally, these results will be used to elicit requirements for the tools and techniques developed within the project.

[1]Throughout this paper I use the term architecture to refer to a set of roles with capabilities to influence each other so that collective behaviour emerges

II. Motivation

Risk is commonly evaluated as the product of the likelihood and impact of an attack. Often though, these cannot be estimated quantitatively, for example because the events are very rare. As such, Risk Assessments are often forced to cope with missing or uncertain data. Even where data is available, it is mostly qualitative.

Security checklists, frequently used to support Risk Assessments, embody experience from the past and are good at detecting and mitigating known risks in an effective manner. However, problems arise when these are used on new or changing architectures or for predicting new types of risks. The rapid proliferation and development of IT systems means that architectures are constantly evolving and what used to be physical systems are now becoming IT systems too. All this raises issues with regard to the identification of new (complex) attacks in the context of a constantly evolving Risk Landscape. To make matters worse, the explosion of virtualized infrastructures (such as clouds) means that even architectures which are already in place are highly dynamic. Furthermore, using such checklists and expert judgement can pose threats to the traceability (and implicitly reproducibility) of such analyses. As such, the growing complexity and diversity of networked applications and critical infrastructures often makes checklists unusable or insufficient.

978-1-4799-3032-6/14/$31.00 © 2014 IEEE

RE 2014, Karlskrona, Sweden

I believe providing argumentation support for these (often informal) assessments, and using architectural models of the system to allow experts to reason about the risks, would facilitate not only the generation of countermeasures (or Security Requirements) but also informative justifications of these. These justifications can serve the purpose of prioritizing countermeasures and providing traceability for security requirements and investments. They can also serve as a basis for future assessments. Argumentation should cope with qualitative, missing or uncertain data by linking qualitative reasoning and quantitative computations.

Another issue is the fact that, in the context of the TREsPASS project, which aims at modelling entire organizations' physical, digital and social domains, factors come into play that were not relevant in traditional assessments. Besides the obvious issue of social engineering attacks, hybrid attacks are also something these methodologies are not very good at tackling. Hybrid attacks imply multiple steps which can include exploiting technical vulnerabilities, bypassing physical controls and applying social engineering techniques in a coordinated attempt to retrieve the desired information. As such, concepts like attacker skill, money flows and collaboration become more relevant and being able to identify or define "attacker business cases" might prove useful in modelling and understanding such complex attacks.

The diversity of systems targeted by Risk Assessments, from consumer applications to cloud infrastructures, means there is a wide variety of (potentially conflicting) requirements for tools and methodologies. These requirements need to be investigated and linked to particular classes of Targets of Assessment in order to provide methods that are better suited to the their application scenarios.

III. Research Questions

The central improvement problem of my research is "How can the process of identifying, analysing, evaluating and ranking relevant Risks in the field of Information Security be improved such that it works with limited or uncertain data, new/complex attacks and changing architectures in order to improve the security investment decision-making process?"

The following sub-research questions can be derived from this central improvement goal:

RQ1 What classes of Target of Assessment for Risk Assessment can be identified?
- RQ1.1 Which architectural views are relevant for each class?
- RQ1.2 What kind of Risk argumentation is feasible for each class?

RQ2 Design improved RA methods for these classes
- RQ2.1 Which RA methods currently exist?
- RQ2.2 What Risk models are implied or defined within these methodologies?
- RQ2.3 What are the drawbacks of current approaches w.r.t. the various classes?
- RQ2.4 What are the requirements for new methods per ToA class?

RQ3 Do the new RA methods produce the desired effects in their intended contexts?
- RQ3.1 Do the new methods satisfy the requirements of each class of system?
- RQ3.2 What metrics and indicators can be used to evaluate and compare the effects across the various contexts?
- RQ3.3 How do the new methods compare to the state-of-the-art w.r.t the identified metrics?

IV. Technical Challenges

I expect to encounter the following technical challenges during the course of this research. I will attempt to treat as many of them as possible during my research, but will focus mostly on the items at the top of the list:

- Finding the right level of formality - too much might over-encumber the analysis, decreasing usability in practice; too little would not allow for (semi-)automated reasoning, decreasing utility in practice.
- Providing traceability and justify-ability of the results - full traceability is not feasible so identifying how much traceability is actually needed in different contexts and how to achieve this sufficient level is important.
- Showing scalability of the approach - the approach has to scale well to larger Information Systems as to cope with the constant expansion of IT systems
- Pushing the boundaries of business modelling languages by using them outside of their intended scope - to describe attacker business cases, parasitic business models, illicit/unintended money flows, etc
- Integrating business modelling concepts into security models in order to reason about attacker goals and means
- Dealing with purely qualitative values and/or lack of quantitative values - as stated in the motivation, quantitative data is frequently lacking but needed for a conclusive assessment; how to work around this?
- Finding out how much of the bookkeeping and verification process can be automated thus reducing the work load of the assessors.
- Providing tool support (usability) - identifying requirements for tools that would support the process and allow for various analyses and computations via an intuitive, easy-to-use interface that can be used by non-experts.

V. State-of-the-Art

A. Information Security Risk and Risk Assessment

The Open Group's "Requirements for Risk Assessment Methodologies" [3] is a useful starting point as it lists high-level, empirically validated requirements that any Risk Assessment methodology should satisfy.

A literature review of current approaches [1] revealed the following potentially useful methodologies:

- FAIR [4], [5], [6], [7] methodology - One of the few methodologies that also comes with an explicit conceptual framework of Risk. Furthermore, it is part of the The Open Group's Standard for Risk Taxonomy [8])

- ISO 2700x [9], [10], [11] series of Information Security standards - currently the most important and recognized standards for Information Security; can provide useful background on current approaches.
- Structured Risk Assessment [12] methodology - unique approach to Risk Assessment, prioritizing simplicity and scalability by imposing a strict structure of the process.
- TARA [13] (Intel) methodology - claims to mitigate the issue of scalability by defining and prioritizing threat profiles; relevant due to the novel approach to describing threat classes.
- other Risk Assessment methodologies and taxonomies will also be analysed and compared.

B. Argumentation

Previous work by Toulmin [14], [15] describes inter- and intra-argument structures at a generic level. It also provides background and in-depth discussions on the uses of argument in various contexts.

The ASPIC+ argumentation framework and related work by Prakken [16] are first steps towards formal implementations of argumentation in security. However, its strict syntax raises issue w.r.t to scalability and ease-of-use.

Previous attempts at using semi-formal argumentation to justify Security Requirements mostly consist of OpenArgue [17] and related work by Haley [18], [19], [20], Franqueira and Nuseibeh [21]. While promising, these approaches are not flexible enough to handle the diversity of ToA's. Furthermore, they have not been shown scalable in practice.

C. Business Models

The e3value ontology [22], a business value modelling language, provides some of the functionality needed in order to describe Risks in Telecom scenarios. These risks are mostly misuse cases, where legitimate users make unexpected, but legal use of Telecom services in such a way that they make a profit, while causing loss for the Providers. The e3value toolkit allows modelling money and service flows and is promising in describing and identifying such Risks.

VI. Solution Directions

Given the problems listed in the Motivation section, I believe that, while a Risk Assessment meta-model can be defined, there is a need for different techniques in order to deal with different classes of Target of Assessment.

I plan to use concepts from rhetoric and argumentation to support the Risk Assessment brainstorming process in order to improve cross-expert agreement, consistency of results and traceability of countermeasures while ultimately providing semi-automated reasoning. The main goal of this research is to find a feasible mix between formal logic and informal argumentation when reasoning about Risks in networks.

In order to achieve trace-ability to a component level, architectural models are needed. For each class of ToAs however, some architectural views provide more useful information than others. So far I have concluded that for traditional IT systems, diagrams of the physical architecture are most useful, but for cases like Telecom fraud, these become largely irrelevant and sometimes impossible to obtain. As such, I use business modelling ontologies to represent and analyse business cases for attackers in contexts where traditional communication diagrams are not effective. I have yet to identify a suitable architectural view for virtualised infrastructures.

I implemented an initial proof-of-concept for conducting argumentation-based RA using spreadsheets. The approach used Toulmin-style arguments in a semi-formal way to identify attack vectors and elicit security requirements for an IPTV-based system and a virtualised infrastructure. Network diagrams were to support the process. As mentioned above, initial results show applicability of such models is limited in the case of virtualised infrastructures.

I have used the e3value business modelling ontology to make business models for the attacker and defender in a couple of Telecom fraud scenarios. Except for the economic actors involved, each model shows which services or monetary transactions occur in the network in the contract period. The models also allow for spreadsheets to be generated showing break-even points for the provider and the fraudster.

VII. Research Contributions

My core theoretical contribution will be knowledge about different classes of Targets of Assessment and RA requirements for each. A secondary contribution lies in exploring the capabilities of informal (Toulmin) and formal (ASPIC+) argumentation framework in analysing Information Security Risks by comparing them with established RA methodologies and using them in conjunction with various types of architectural views. Furthermore, it pushes the limits of business modelling languages, drawing conclusions on their sensitivity and extensibility while proposing new ways of using them in order to describe and hopefully identify Risks.

By extending argumentation theory with a conceptual model of Risk and identifying suitable architectural views to support this for various types of systems, I hope to improve the traceability and flexibility of Risk Assessment methodologies. As such, the practical relevance is that we will be able to do better RAs for a larger diversity of ToAs.

VIII. Research Methods

I have conducted a literature study and review of the state-of the art to identify current approaches (RQ2.1, RQ2.2). Case studies and Technical Action Research with the industrial partners of the TREsPASS project will be used to identify limitations of these in various contexts and requirements for improvement (RQ2.3, RQ2.4).

I will then carry out multiple iterations of Case Studies and Technical Action Research with both established and experimental RA methods in various specific scenarios (like IPTV, Cloud, Telecom) and in conjunction with various modelling languages as to identify which architectural views are more useful for each scenario (RQ1). For the initial prototypes

students will be used. Later, cross-expert evaluation will be employed to assure re-usability.

I will finally attempt to design a new set of methods and guidelines (and possibly tool) to advance the current state of the art. I will use Metric Definition Approaches (like GQM/MEDEA) to identify suitable indicators that can be used to evaluate the measure to which the goals were reached and to compare the new method(s) to established methodologies (RQ3.1, RQ3.2). Proven techniques like Gorschek's Model for Technology Transfer [23] and Wieringa's approach to scaling up to practice [24] will be used to validate the new method(s) both within the TREsPASS project and externally via TAR(RQ3.2).

IX. Progress

I started off by conducting a structured literature survey of current established Risk Assessment frameworks, methodologies, tools and standards in order to get familiar with the state-of-the-art. As indicated in the Research Methods, I also conducted several initial case studies and Risk Assessments using established methodologies in order to identify potential limitations and requirements:

- Case study and Risk Assessment of the "Follow-me" printing infrastructure of the University of Twente following the Australian/New Zealand Standard for Risk Management
- Case study and Risk Assessment of BYOD implementation in an SME based on industry guidelines (in the lack of other suitable established methodologies)
- Case study and Risk Assessment of IPTV-based home payments prototype according to the Structured Risk Assessment methodology

Initial progress towards designing a new solution so far includes:

- Experiment in using formal logic framework (ASPIC+) to support Risk Assessment with Prakken[16]
- Spreadsheet-based tool and proof-of-concept aiming at a middle ground between Prakken's formal approach [16] and OpenArgue's less formal method [17].
- Applying the e3value ontology to model business cases for malicious users in several Telecom fraud scenarios.

The following were carried out in order to validate the initial solutions:

- Case Study and Risk Assessment of generic IaaS Cloud infrastructure with IBM Research Zurich using the spreadsheet-based tool and public Cloud Risk knowledge bases [25], [26]
- Multiple case studies and Risk Assessments of IPTV home-payments system using the spreadsheet-based tool
- Collaboration with the Deutsche Telekom Chair of Mobile Business & Multilateral Security for validating the e3value approach in Telecom misuse scenarios

X. Accepted Publications

- H. Prakken, D. Ionita, and R. Wieringa, "Risk assessment as an argumentation game" in *Computational Logic in Multi-Agent Systems*. Springer Berlin Heidelberg, 2013, pp. 357373.

References

[1] D. Ionita, *Current established risk assessment methodologies and tools*, July 2013. [Online]. Available: http://essay.utwente.nl/63830/

[2] "Technology-supported risk estimation by predictive assessment of socio-technical security," 2012-2016. [Online]. Available: https://www.trespass-project.eu/

[3] T. O. Group. (2009, January) Requirements for Risk Assessment Methodologies.

[4] R. M. I. LLC, *FAIR (FACTOR ANALYSIS OF INFORMATION RISK) Basic Risk Assessment Guide*. Risk Management Insight LLC, 2006.

[5] T. O. Group, *Technical Guide: Fair - ISO/IEC 27005 Cookbook*, October 2010, no. C103.

[6] R. M. I. LLC, *FAIRLite High-Level Description*. Risk Management Insight LLC, 2010.

[7] J. A. Jones, "An Introduction to Factor Analysis of Information Risk (FAIR)," Risk Management Insight, 2005.

[8] T. O. Group, *Technical Standard to Risk Taxonomy*, January 2009, no. C081.

[9] "Information technology – Security techniques – Information security management systems – Requirements," 2005.

[10] "Information technology – Security techniques – Code of practice for information security management," 2005.

[11] "Information technology – Security techniques – Information security risk management," 2011.

[12] N. A. McEvoy and A. Whitcombe, "Structured risk analysis," in *Proceedings of the International Conference on Infrastructure Security*, ser. InfraSec '02. London, UK, UK: Springer-Verlag, 2002, pp. 88–103.

[13] M. Rosenquist, "Prioritizing information security risks with threat agent risk assessment," "http://www.communities.intel.com/servlet/JiveServlet/download/4693-1-3205/Prioritizing_Info_Security_Risks_with_TARA.pdf", December 2009.

[14] S. E. Toulmin, *The Uses of Argument*. Cambridge University Press, July 2003.

[15] S. Toulmin, R. Rieke, and A. Janik, *An introduction to reasoning*. Macmillan, 1979.

[16] H. Prakken, D. Ionita, and R. Wieringa, "Risk assessment as an argumentation game." in *CLIMA*, ser. Lecture Notes in Computer Science, J. Leite, T. C. Son, P. Torroni, L. van der Torre, and S. Woltran, Eds., vol. 8143. Springer, 2013, pp. 357–373.

[17] Y. Yu, T. T. Tun, A. Tedeschi, V. N. L. Franqueira, and B. Nuseibeh, "Openargue: Supporting argumentation to evolve secure software systems." in *RE*. IEEE, pp. 351–352.

[18] C. Haley, R. Laney, J. Moffett, and B. Nuseibeh, "Security requirements engineering: A framework for representation and analysis," *IEEE Trans. Softw. Eng.*, vol. 34, no. 1, pp. 133–153, Jan. 2008.

[19] C. B. Haley, R. C. Laney, B. Nuseibeh, W. Hall, C. B. Haley, R. C. Laney, and B. Nuseibeh, "Validating security requirements using structured toulmin-style argumentation," 2005.

[20] R. M. J. D. Haley, Charles B; Laney and B. . Nuseibeh, "Arguing satisfaction of security requirements."

[21] V. N. L. Franqueira, T. T. Tun, Y. Yu, R. Wieringa, and B. Nuseibeh, "Risk and argument: A risk-based argumentation method for practical security." in *RE*. IEEE, 2011, pp. 239–248.

[22] J. Gordijn and H. Akkermans, "Value based requirements engineering: Exploring innovative e-commerce idea," *Requirements Engineering Journal*, vol. 8, no. 2, pp. 114–134, 2003.

[23] T. Gorschek, P. Garre, S. Larsson, and C. Wohlin, "A model for technology transfer in practice," *IEEE Software*, vol. 23, no. 6, pp. 88–95, 2006.

[24] R. J. Wieringa, "Empirical research methods for technology validation: Scaling up to practice," *Journal of systems and software*, vol. online pre-publication, 2014.

[25] "ENISA: Cloud Computing Security Risk Assessment," May 2009. [Online]. Available: http://www.enisa.europa.eu/pages/02_03_news_2009_05_18_risk_survey.html

[26] "Top Threats to Cloud Computing V1.0," 2010.