Visual Analytics for Requirements-driven Risk Assessment

Robin A. Gandhi and Seok-Won Lee
Dept. of Software and Information Systems, The University of North Carolina at Charlotte
Charlotte, NC 28223-0001, USA. {rgandhi, seoklee}@uncc.edu

Abstract

Risk assessment is a complex decision making process during Certification and Accreditation (C&A) activities. It requires to understand the multi-dimensional correlations among numerous C&A requirements to reason about their collective and adequate behavior to minimize risks to a software system. Also, diverse stakeholders in the organizational hierarchy should be able to comprehend and utilize the risk assessment artifacts to agree upon an acceptable level of risks and justify the criticality and cost of mitigation strategies related to C&A requirements. We believe requirements visualization plays an important role in providing rich contextual information for understanding and analyzing risk assessment artifacts and present our initial experiences in using intuitive visual metaphors and their explanations for requirements-driven risk assessment [8] [11].

1. Introduction

Security certification establishes the extent to which a particular design and implementation meets a set of specified security requirements (usually referred to as baseline security controls) [4]. Standardized C&A requirements reflect organizational concerns for security risks most critical in their environment. Operational profiles [19] and use cases [6] are also necessary to assess security risks. Therefore, the organization's confidence on its software systems to reliably support its critical businesses/missions is assured when these risks are demonstrated to be reduced to an acceptable level. To make such assessment, following certification, the goal of accreditation is to agree upon an "*acceptable level of risk*" for authorizing system operation as shown in Figure 1. However, given the complexity of current software systems and numerous C&A requirements, a thorough assessment of risks is very difficult.

Infrastructure-wide standard security C&A requirements are tailored according to the unique socio-technical environment of an organization. However, C&A requirements are usually specified in ambiguous natural language descriptions and scattered across multiple regulatory documents that express diverse stakeholders' viewpoints in the organizational hierarchy. As a result, a great deal of subjectivity is involved in understanding C&A requirements and assessing the impact of evidences gathered for their compliance on the emergent system behavior. These issues greatly undermine the ability of certification analysts to make objective decisions about acceptable levels of risks and making recommendations about authorizing system operation. In turn, system stakeholders often find it difficult to comprehend and utilize the risk assessment artifacts (usually thick reports with technical details) from C&A activities.

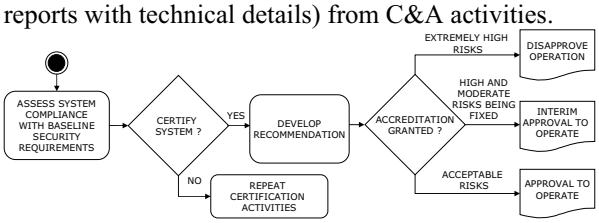

Figure 1: Certification and Accreditation Activities

To address these issues, we explore the possibilities of performing visual analytics [20] [17] within our integrated methodology for requirements-driven risk assessment [8] [11]. Specifically, we use requirements visualization techniques to illustrate the risks due to cascading effects of non-compliance with C&A requirements on system behavior. Different visual metaphors and explanations are intended to support certification analysts in effectively focusing on critical C&A requirements for assessing risks in a given operational scenario. Findings from our approach applied to a regulatory C&A process of The United States Department of Defense (DoD) are presented.

2. Background

2.1 Modeling C&A Requirements

Guided by the Ontology-based ACTive Requirements Engineering (Onto-ActRE) framework [10], we harness the expressiveness of ontologies to classify and categorize C&A requirements from the following dimensions: 1) a requirements domain

Second International Workshop on Requirements Engineering Visualization (REV 2007)
978-0-7695-3248-6/07 $25.00 © 2007 IEEE

model of requirement types that hierarchically categorizes C&A requirements; 2) a viewpoints hierarchy that models different perspectives and related stakeholders of a C&A requirement; 3) a C&A process goal hierarchy with leaf-node scenarios to express process activities related to a C&A requirement; and 4) domain-specific taxonomies of risk components of assets, threats, vulnerabilities, and countermeasures related to C&A requirements. Currently, the Onto-ActRE framework has been applied to the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) [3] [4] to build a Problem Domain Ontology (PDO) by processing approximately 800 pages of regulatory documents.

As compared to ambiguous natural language specifications that are open to subjective interpretation, the semantics of each DITSCAP requirement is now established by visualizing its relationships with other domain concepts in the DITSCAP PDO. For example, Figure 2 visualizes the DITSCAP requirement of "Remote Access Audit Trails for Privileged Functions" [5] and its relationships in the DITSCAP PDO to precisely establish its semantics among stakeholders. The DITSCAP PDO includes 604 domain concepts that help to understand 533 C&A requirements. Further details can be found in [12] [15] [13].

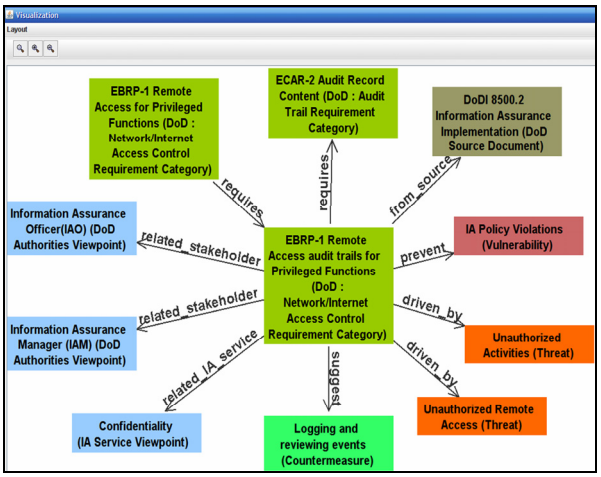

Figure 2: Visualizing a C&A Requirement

2.1.1 C&A Requirements & Risk Components

To systematically identify and reason about the risk components expressed (or missing) in natural language C&A security requirements descriptions, we extend the Common Criteria security model [2]. The resulting model, as shown in Figure 3, explains the relationships between security requirements and risk components.

Based on the model in Figure 3, a domain expert identifies the relevant risk components and maps them to the concepts in the domain-specific taxonomies of threats, assets, vulnerabilities, and countermeasures modeled in the PDO. Processing a C&A requirement description involves various heuristics based on domain expertise, keyword analysis, regulatory document exploration, hierarchical browsing of concepts and navigating their relationships in the PDO.

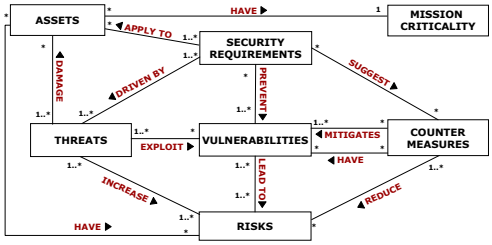

Figure 3: Requirements and Risk Model [8]

2.1.2 Evidences for Requirements Compliance

For each C&A requirement, the PDO development involves the creation of structured "compliance questionnaires" by a domain expert who has many years of experience in the field of performing C&A. Each question has well-defined answer options that reflect the following ordered levels of compliance: 1) fully compliant; 2) partially compliant; 3) non-compliant; and 4) no evidences, for ease and uniformity in interpretation.

3. Visual Analytics for Risk Assessment

Security risks in a complex system most often arise due to cascading effects of a failure (e.g. weakest link syndrome) among security constraints that collectively contribute to emergent secure software behavior. As a result, from a C&A perspective, discovering and understanding the multi-dimensional correlations among different classes of security constraints imposed in the operational context of a complex software system is necessary to uncover and assess all possible risks. To this end, requirements visualization will play an important role in providing additional context for risk assessment as a decision making process based on multi-dimensional analysis in the problem domain.

We present a step-wise methodology in [8] for discovering and understanding the correlations among C&A requirements applicable in a given operational scenario of the target system to conduct risk assessment. While specific details of our methodology can be found in [8], here we briefly discuss the characteristics of the resulting visual risk assessment artifacts based on Formal Concept Analysis (FCA) [9]. Brief introduction to FCA can also be found in [8].

A *formal context* for conducting FCA is built from an *Analysis Pool* of C&A requirements. We define analysis pool as an exhaustive compilation of C&A requirements that collectively constrain target system

978-0-7695-3248-6/07 $25.00

behavior in diverse ways in a socio-technical environment for a given operational scenario. A stepwise process of selecting the C&A requirements to be included in an analysis pool; and then, their abstraction to requirement categories modeled in the PDO is required to build a *formal context.* The *formal context* is then represented as a cross table with one row for each C&A requirement category (*formal object)* and one column for each risk component (*formal attribute)* by having a cross in the intersection of row and column if the corresponding C&A requirement category and risk component are related in the PDO. The *formal context* is also augmented based on the "is-a" relationships among C&A requirements categories or risk components in the PDO.

Within the *formal context*, a *formal concept* is defined as a pair of sets (A, B); where A is a set of C&A requirements categories called its extent (connections to reality); and B as a set of risk components called its intent (semantics). A *formal concept* (A, B) is a subconcept of a *formal concept* (C, D), if the extent A is a subset of the extent of C or if the intent of B is a superset of the intent of D. The partially ordered set of all *formal concepts* is always a complete lattice structure and is called a *concept lattice*. An example concept lattice for a hypothetical remote access target system operational scenario is shown in Figure 4 (Reproduced from [8]).

The concept lattice provides a visual and concise representation of all potential correlations among C&A requirements categories in the given scenario, while facilitating their interpretation for risk assessment. The most general node that covers all risk components related to a requirement category is labeled with that requirement category. The most specific node that covers all requirement categories related to a risk component is labeled with that risk component. For a node in the lattice, the extent of the corresponding *formal concept* includes all the requirements categories that are reachable in the lattice navigating downward from the node (including the selected node). The intent of the *formal concept* includes all the risk components that are reachable in the lattice navigating upward from the node (including the selected node).

3.1 Formal Concept Explanations

For ease of understanding the *formal concepts* in a lattice, their natural language explanations are automatically generated by interpreting their intent, extent, and their relationships based on the requirements and risk model in Figure 3. Example explanation of the node "C15" is shown in Figure 4. The explanations "*restore*" the meaning of relationships between requirements and risk components, which were previously recorded only as "crosses" in a *formal context* cross table, based on the domain semantics of the PDO (model of Figure 3).

3.2 Visualizing the Problem Context

The concept lattice provides several metrics for risk assessment [8]; however, computing them requires keen visual inspection of the lattice structure. The lattice also lacks information about the requirements compliance levels in the context of the target system. Therefore, to augment the analytical capabilities of the concept lattice for risk assessment, we have developed

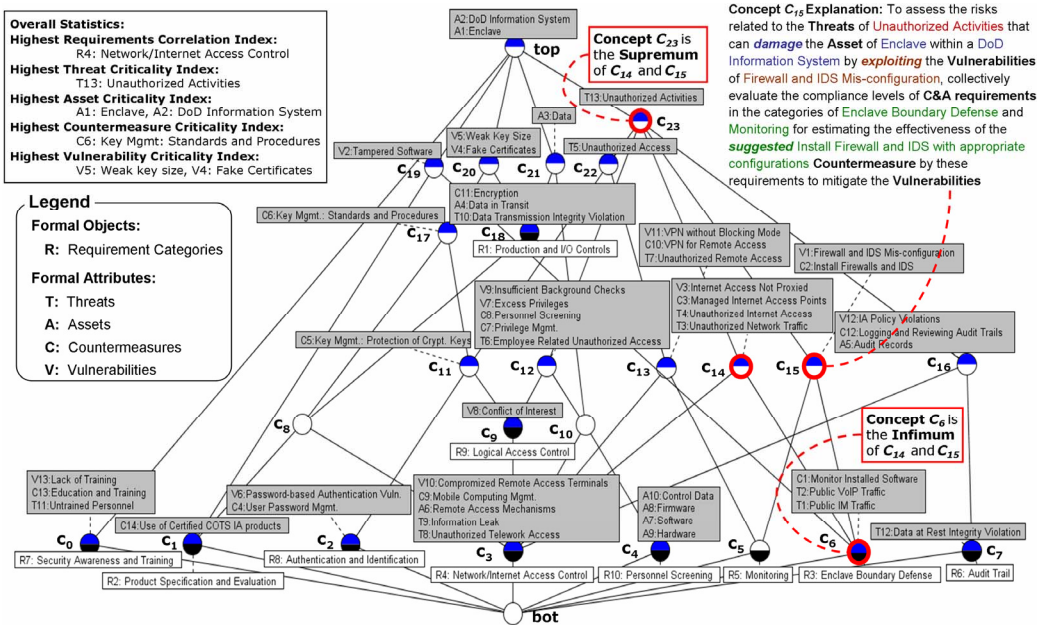

Figure 4: An Example Concept Lattice for Remote Access Operational Scenario of the Target System [8]

978-0-7695-3248-6/07 $25.00

visual metaphors that can illustrate critical requirements and the potential risks due to cascading effects of their non-compliance on overall system behavior. Visual features of the metaphors convey metrics derived from the concept lattice [8], metrics gathered from requirements compliance questionnaires (section 2.1.2), and semantics derived from the PDO (the understanding of C&A requirements and related risk components, e.g. Figure 2).

3.2.1 Visual Metaphor: Cohesive Bar Graph. A *formal concept*, in our approach, generates cohesion among requirements in its extent based on shared risk components among them in its intent. Therefore, we visualize a *formal concept* based on the "*cohesive bar graph*" visual metaphor as shown in Figure 5. Each bar in the graph represents a *formal object* (requirement category) in the *formal context*.

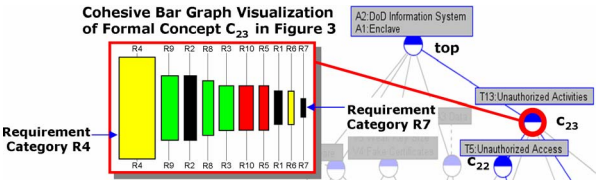

Figure 5: Visual Metaphor: Cohesive Bar Graph

Visual features of a bar represent several quantitative and qualitative metrics for a requirement category:

− **The color of a bar:** It represents the compliance level of the corresponding requirement category in the context of the target system (section 2.1.2). "Green" represents full compliance, "Yellow" represents partial compliance, "Red" represents non-compliance, and "White" indicates absence of evidences. A "Black" bar represents that the corresponding requirements category is not in the extent of the selected node.

− **The height of a bar:** It represents the requirement category correlation index [8]. In the range of [0, 1], it is a ratio of the number of *formal concepts* that cover the requirement category in their extent, and the total number of *formal concepts*. Larger the ratio, higher is the potential for correlation of a requirement category with other requirements categories due to shared risk components in the given scenario.

− **The width of a bar:** It represents the ratio of the number of risk components related to a requirement category in the *formal context*, and the total number of risk components in the *formal context*. Larger the width of a bar for a requirement category, higher is its coverage of risk components in the given scenario.

− **The ordering of bars:** It is based on height and then based on width (for bars with the same height). The ordering and the color of the bars now help to readily prioritize requirement categories for their influence on the risk components in the intent of the *formal concept* based on their potential to correlate with other requirements, coverage of risk components, and their level of compliance in the given scenario.

3.2.2 Impact Analysis using Cohesive Bar Graph. The goal of impact analysis is to identify a set of requirements categories, in addition to the known non-compliant requirements categories, whose compliance will be potentially undermined and then to reveal all the corresponding potential risks in the scenario. Adopting the techniques in [18], such analysis can be visually conducted as follows: 1) Identify the most specific *formal concept* in the concept lattice, that contains all the non-compliant requirement categories in its extent; and then 2) For the identified *formal concept*, all its *super-concepts* (and the requirement categories in their extent) in the lattice are investigated for potential propagative effects of non-compliance.

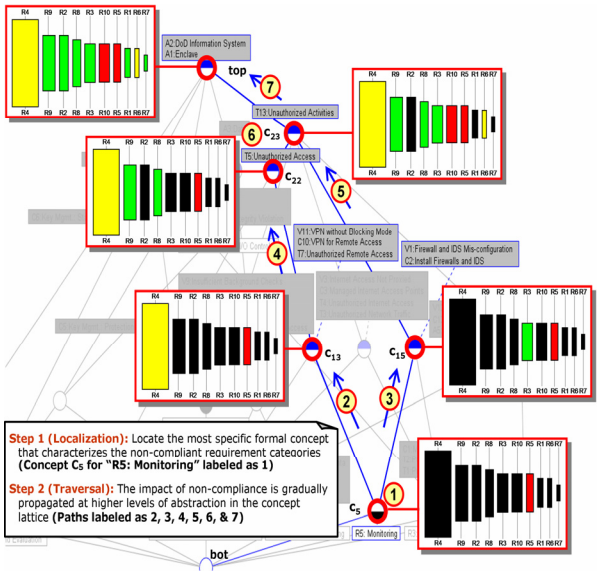

Figure 6: Non-Compliance Impact Analysis

Figure 6 shows an example impact analysis for non-compliance in the "R5: Monitoring" requirement category of Figure 4. Traversing the *super-concepts* of the *formal concept* that characterizes "R5: Monitoring" in the concept lattice creates a logical and hierarchical argument structure that helps to systematically reason about the potential propagative effects of non-compliance among requirement categories in the given scenario. During traversal, each *super-concept* and the requirement categories in its extent are examined by a certification analyst to identify potential cascading effects of non-compliance in the context of the target system. To this end, visual features of the cohesive bar graph can reduce the cognitive overload on the certification analyst by visualizing the metrics available for each requirement category in the extent of a *formal concept*. Traversal of the cohesive bar graphs

978-0-7695-3248-6/07 $25.00 © 2007 IEEE

at different levels of abstraction promotes a gradual discovery and learning process to unravel the propagative effect of non-compliance.

3.2.3 Visual Metaphor: Cohesive Arc Graph. It is useful to visualize the *degree of influence* a given requirement category will have on the effective implementation of other requirement categories in a given scenario. Therefore, we use the "*cohesive arc graph*" visual metaphor (adopted from [16]) as shown in Figure 7. The requirement category of interest is arranged in the middle as a circle. Each arc around the circle corresponds to a requirement category in the current scenario other than the one in the middle, and its visual features represent the following metrics:

− **The color of an arc:** Represents the compliance level of the requirement category (as in section 2.1.2)

The radius of an arc: It reflects the *requirement influence factor* (RIF) metric. RIF is a ratio of the number of *formal concepts* shared between the requirement category in the middle and the requirement category represented by the arc and the total number of *formal concepts* that cover either of the two requirement categories in their extent. Higher the RIF, higher are the similarities of two requirement categories in correlating with other categories in the given scenario. RIFs allow perceiving the criticality of a requirement category to strengthen the level of compliance with a large proportion of requirements in the given scenario. Figure 7 visualizes the RIFs for the "R5: Monitoring" requirement category. It adds value to the analytical abilities for impact analysis in Figure 6.

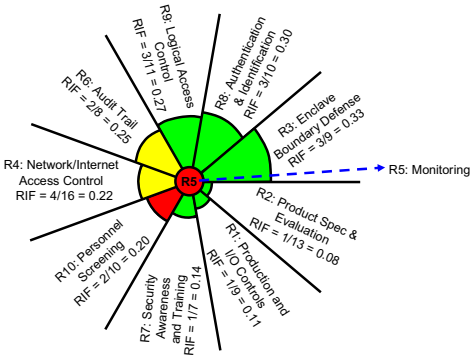

Figure 7: Cohesive Arc Graph Visualization of RIF

4. Discussion

The feasibility of producing the visualizations has been demonstrated in the initial implementation of the C&A workbench [11] [14]. Their usefulness has been evaluated as part of a larger case study with C&A experts, where the visual metaphors were found to be particularly useful to understand the risk assessment artifacts from FCA. A more elaborate discussion of these results will be a part of our future publications.

Benefits of visualizations for compliance management [1], and to support quantitative risk-based decision processes to illustrate cost-effective design solution spaces [7] have been observed. Our techniques complement these approaches by providing capabilities to understand the large and unstructured space of C&A requirements, their applicability, and their compliance levels and associated risks in the context of a complex system. In the future, we will investigate more interactive visualizations of C&A requirements spaces and related evidences that promote software assurance among stakeholders.

5. References

[1] Bellamy, R.K.E., Erickson, T., et al, "Seeing is believing: Designing visualizations for managing risk and compliance" IBM Systems Journal, 46(2), Compliance Management, 2007, pp. 205

[2] Common Criteria, Ver. 2.1. ISO/IEC 15408-1, 1999

[3] DoD 8510.1-M: DITSCAP Application Manual. 2000

[4] DoD Instruction 5200.40: DITSCAP, 1997.

[5] DoDI 8500.2. IA Implementation. Feb 2003.

[6] Donzelli, P., Basili, V., "A practical framework for eliciting and modeling system dependability requirements," Journal of Systems and Software, Vol. 79(1), 2006, pp. 107-119.

[7] Feather, M.S., Cornford, S.L., et al, "Experiences using Visualization Techniques to Present Requirements, Risks to Them and Options for Risk Mitigation," REV 06, 14th RE, 2006, p. 10

[8] Gandhi, R. A. and Lee, S. W., "Discovering and Understanding Multi-dimensional Correlations among Certification Requirements with application to Risk Assessment", To appear in Proc. of the 15th IEEE Int'l RE Conf. (RE 07), October 15-19, Delhi, India, 2007.

[9] Ganter, B., Wille, R. *Formal Concept Analysis*. Springer, 1996

[10] Lee, S.W., Gandhi, R. A., "Ontology-based Active Requirements Engineering Framework," In Proc. 12th Asia-Pacific Soft. Engg. Conf. (APSEC 05), IEEE CS Press, 2005, pp. 481-490.

[11] Lee, S.W., Gandhi, R.A. et al. "r-AnalytiCA: Requirements Analytics for Certification & Accreditation," To appear in Proc. of 15th IEEE Int'l RE Conf. (RE 07), Posters, Demos and Exhibits Session, October 15-19, Delhi, India, 2007.

[12] Lee, S.W., Gandhi, R.A., "Requirements as Enablers for Software Assurance," CrossTalk: The Journal of Defense Software Engineering, December Issue, 19(12), 2006, pp. 20-24.

[13] Lee, S.W., Gandhi, R.A., Ahn, G.J., "Certification Process Artifacts Defined as Measurable Units for Software Assurance" Soft. Process: Improvement and Practice, Vol. 12(2), 2007, pp. 165-189.

[14] Lee, S.W., Gandhi, R.A., and Wagle, S.J., "Towards a Requirements-driven Workbench for Supporting Software Certification and Accreditation," In Proc. of the 3rd Int'l Workshop on Soft. Engg. for Secure System (SESS 07), at ICSE 07, 2007.

[15] Lee, S.W., Muthurajan, D., Gandhi, R.A., et al., "Building decision support problem domain ontology from natural language requirements for software assurance," Int'l Journal on Software Engg. and Knowledge Engg., 16(6), Dec. 2006, pp. 851-884.

[16] Schedl, M., Knees, P., Widmer, G., "Interactive Poster: Using CoMIRVA for Visualizing Similarities Between Music Artists," 16th IEEE Visualization Conference (VIS '05), 2005, p. 89

[17]Thomas, J.J. Cook, K.A. (eds.), "Illuminating the Path: The Research and Development Agenda for Visual Analytics," 2005.

[18] Tonella, P., "Using a concept lattice of decomposition slices for program understanding and impact analysis," IEEE TSE 29(6), 2003.

[19]Voas, J., "Certifying software for high-assurance environments," IEEE Software, Vol.16 (4), Jul/Aug 1999, pp.48-54.

[20]Wong, P.C., Thomas, J., "Visual Analytics," IEEE Computer Graphics and Applications, Vol. 24(5), 2004, pp. 20- 21.

978-0-7695-3248-6/07 $25.00 © 2007 IEEE