Ontology Guided Risk Analysis: From Informal Specifications to Formal Metrics

Robin Gandhi and Seok-Won Lee

Abstract. The level of compliance with security certification requirements is the primary driver of the decision to accredit a software system into operation with an acceptable level of risk. However, given the complexity of current software systems, numerous natural language Certification and Accreditation (C&A) requirements, and ad-hoc processes to assess compliance, this decision is often based on the subjective judgment of the designated officials rather than well-designed metrics and measures. This chapter presents our ongoing research on ontology guided process of building "formal metrics" for understanding risk from the informal specification of security requirements and related evidence collected from the C&A process. The transformation of informal sources (in the problem space) into a representation that supports well-defined metrics (in the solution space) is realized through a combination of knowledge engineering and requirements engineering techniques. Our research outlines a methodological approach for metrics development and understanding using the structured representation of regulatory security requirements in a problem domain ontology. The metrics derived from the domain ontology create a traceable chain of analytical thoughts with software artifacts (e.g. requirements, design, and code). We provide concrete examples for the feasibility of our research findings through its application to a security C&A process and the resulting tool suite.

Keywords: Risk Analysis, Security Requirements, Metrics, Certification and Accreditation, Ontology based Conceptual Modeling, Traceability.

Robin Gandhi
University of Nebraska at Omaha, College of Information Science and Technology,
6001 Dodge Street, Omaha, NE 68182,
email: rgandhi@unomaha.edu

Seok-Won Lee
University of North Carolina at Charlotte, College of Computing and Informatics,
9201 University City Blvd., Charlotte, NC 28223,
email: seoklee@uncc.edu

Z.W. Ras and W. Ribarsky (Eds.): Advances in Information & Intelligent Sys., SCI 251, pp. 227–249.
springerlink.com

1 Introduction

The notion of "Risk" is shaped by the security needs in a problem domain, thus, contextually subjective. From a governance perspective, the security needs are often expressed as a standard baseline of security requirements enforced through regulatory processes such as Certification and Accreditation (C&A). Infrastructure-wide standard C&A requirements are tailored according to the unique socio-technical environment of an organizational infrastructure and embody the security needs as understood in that problem domain. In turn, the C&A requirements reflect organizational concern for risks most critical in their socio-technical environment. Therefore, an organization's confidence in its software systems to reliably support critical businesses/missions is assured when these risks are demonstrated to be reduced to an acceptable level. The complexity of current software systems and their socio-technical environments demand that such confidence should be based on metrics and measures from multiple dimensions addressed by C&A requirements and their interdependencies with each other.

Putting the C&A process into practice is not easy. It is a long and exhaustive manual process of collecting evidence from the target system to assess the level of compliance with numerous C&A requirements. Furthermore, natural language C&A requirements have little or no structural regularity in their specifications. Numerous C&A requirements are scattered across many guidance documents which reflect stakeholder interests from various levels in the organization. From a compliance assessment perspective, security requirements are generally hard to test and measure their effectiveness. Security is an emergent property of the system as a whole and generally cannot be verified by mere inspection of individual components in a large and complex system. The combination of these factors greatly undermine the ability of certification analysts to make objective decisions about an acceptable level of risk using evidences gathered for compliance with C&A requirements. Therefore, in our research efforts, we have developed a systematic framework [28] to model C&A requirements using a combination of knowledge engineering and requirements engineering techniques [27] [25]. A common language enabled by this framework supports the development of metrics and measures in diverse dimensions as well as examines their interdependencies to understand potential risks [16].

The development of complex and socio-technical systems requires many different kinds of metrics and measures for different purposes, stakeholders, standards, and functionalities. Socio-technical environments typically entail interactions between software, hardware, people, data, physical spaces, organizational policies, standards, procedures, laws, and regulations. Naturally in such multi-faceted environments, emergent security properties are inherently difficult to understand, assess, control and predict. To manage this complexity with possibly diverse set of information sources, rather than relying on any single modeling philosophy or notation, in our framework [28], we explicate each C&A requirement based on attributes that capture the goals, scenarios, viewpoints and other domain-specific concepts necessary for precisely establishing their semantics in a Problem Domain Ontology (PDO).

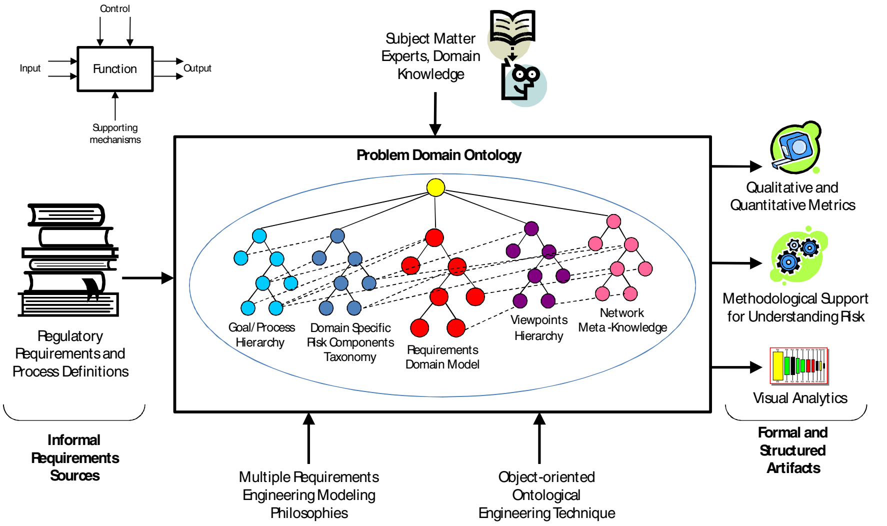

Control
Input
Function
Output
Supporting mechanisms
Subject Matter Experts, Domain Knowledge
Problem Domain Ontology
Goal/Process Hierarchy
Domain Specific Risk Components Taxonomy
Requirements Domain Model
Viewpoints Hierarchy
Network Meta-Knowledge
Regulatory Requirements and Process Definitions
Informal Requirements Sources
Multiple Requirements Engineering Modeling Philosophies
Object-oriented Ontological Engineering Technique
Qualitative and Quantitative Metrics
Methodological Support for Understanding Risk
Visual Analytics
Formal and Structured Artifacts

Fig. 1 Overview of Ontology guided Transformation of Informal Requirements Sources into Formal and Structured Artifacts

Our approach to ontology development is primarily problem driven. Its creation is guided based on the problem solving notions in multiple complementary requirements engineering techniques that effectively characterize the security needs from different dimensions. The resulting integrated ontology is a human and machine understandable, hierarchical model of security needs, engineered using object-oriented ontological domain modeling techniques [27].

In this chapter, we summarize our experiences in using ontology development and associated analysis techniques for understanding risk in the operational context of a software system. The transformation of informal security C&A requirements specifications into formal metrics and visual metaphors for understanding risk is a novel approach and a key contribution of our research. Fig. 1 depicts this ontology guided transformation of natural language security C&A requirements and process guidance documents into formal and structured artifacts that help to understand risk during the C&A process.

Our general framework has been applied to the C&A process within the United States Department of Defense (DoD) organization. In the DoD problem domain, security is a key dependability attribute for software systems that provide an infrastructure for local and global DoD information needs. The standard DoD Information Technology Security Certification and Accreditation Process (DITSCAP) [13] [12] ensures that the DoD security needs are uniformly considered and maintained throughout the lifecycle of all information systems that support information processing services within the DoD information infrastructure (DII). Essentially, DITSCAP provides a management infrastructure for gathering metrics and measures which can be used to guide as well as assess secure software engineering activities. We elaborate on various aspects of our approach using examples in the DITSCAP domain.

Organization of the rest of the chapter is as follows. Section 2 discusses related work in this area followed by a brief overview of the DITSCAP PDO resulting from our previous research efforts in section 3. Section 4 outlines the PDO driven development of a diverse set of metrics and measures to understand risks in the operational context of a software information system subject to the DITSCAP. We then discuss the end-to-end traceability of specific and technically inclined Information Assurance (IA) metrics to the visual metaphors related to regulatory requirements and risk components in a complex socio-technical environment. In section 5 we discuss the manifestation of our approach in a C&A tool suite. Finally, in section 6 we provide our concluding remarks and future work.

2 Related Work

Both quantitative and qualitative metrics have been explored extensively to understand risk to software systems. Quantitative risk assessment approaches follow the general philosophy of listing potential threats/failures in a system, quantifying the effect of each identified threat/failure on the assets, and then prioritizing each potential threat/failure according to its severity. Consequently, the accuracy of risk estimates obtained using quantitative methods relies heavily on the rigor in identifying all potential risk components and their interactions within the bounds of investigation. Despite the mathematical rigor in quantitative methods, inaccurate description of the real-world phenomena will only produce more erroneous results. In addition, quantitative measures of risk are most often rough estimates (similar to weather forecasts) or based on expert opinions that rely on qualitative measures. Butler et al. [5] have observed that in addition to quantitative metrics, in practice, the choice of security mechanisms is strongly driven by considerations of diverse non-technical and qualitative measures. The notion of risk being fundamentally subjective, we posit that a combination of both quantitative and qualitative measures to understand risk is inevitable in a socio-technical environment. In this direction, our work provides a baseline for systematically developing rigorous (formal and justifiable) qualitative and quantitative metrics for understanding risk, and analyzing their inter/intra-dependencies driven by regulatory requirements (informal sources) applicable to an organization.

Quantitative risk-centric decision processes [15] [4] rely on knowledge from experts and past experiences/records to perceive potential risks and then prioritize requirements, but lack a baseline for systematically identifying potential risks in a given organizational environment. Qualitative measurement approaches such as Goal Question Metric (GQM) [2] and balanced scorecard framework [22] are frequently used for metric development during the software lifecycle. Their influences are also apparent in approaches for defining security metrics and measures [41] [42] [33]. Taxonomical questionnaires that reflect a refinement hierarchy of qualitative metrics and measures have been proposed for enterprise-level risk assessment [20] [6]. However, these approaches are only focused on the collection of evidence from the software system, but do not help to reveal interdependencies among them in the operational context of the system to understand the true risk potential. Vaughan et al. [46] quote that metrics should be developed as a cross product of what needs to be measured, why you need to measure it, and for whom you measure it. Such alignment of assurance metrics and measures with their real world objectives is a limitation of current practices.

Frameworks for enterprise-level risk assessment, such as the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)) [8], CORAS [1] and Risk Management Framework (RMF) [47], propose their own methodological steps, but lack specific guidelines to interoperate with C&A activities and appropriately utilize the evidences gathered for C&A requirements into the risk assessment process. With increasing system complexities, the criteria for risk assessment is often confined and restricted to the experts in the domain or trained professionals who are familiar with specific standards, operating systems, programming languages and communication protocols. The interdependencies that exist between information from diverse sources significantly restrict human ability to effectively engineer secure systems and identify, evaluate, and report their assurance levels. To further aggravate the situation, C&A processes often reduce to a mere bureaucratic necessity to get approval to operate by generating required documentation, without specific focus on assessing and managing the operational risks of the site and system [11].

Automated tools for assisting secure software engineering activities [36] utilize the available taxonomies of software flaws [48] [44], common vulnerabilities [10], and reference data sets [39] to produce many metrics and measures. But, these metrics and measures lack the traceability to and context of their related security requirements and real-world needs of the business/mission. As a result, the C&A process and associated risk assessment fail to appropriately consider the evidence grounded in the specific operational environment or technical attributes of the software system.

Requirements engineering makes extensive usage of conceptual modeling [21] [38] as a means to comprehend, communicate and analyze the requirements of the system to be developed in its environment. With requirements manifest only in the problem domain [19], requirements engineering techniques that facilitate problem domain understanding and communication between stakeholders also suggest intuitive metric categories from diverse dimensions. Popular requirements engineering techniques based on the notions of goals [45], viewpoints [24] and scenarios [40] share many similarities with conceptual aids for metric development. These notions facilitate elicitation, modeling and analysis of requirements and related domain knowledge expressed using a lexicon accessible to the involved stakeholders. In our research, we have effectively combined these notions using ontology building techniques to derive metrics and measures that are highly intuitive for the stakeholders of the C&A process to understand risk.

The SQUARE [34] methodology, for eliciting, categorizing, and prioritizing security requirements, define risk assessment as a part of their process steps. However, the selection of a technique for risk assessment is left entirely up to the analyst, leading to loose integration with other steps in the requirements engineering process. In [35], the need for integrating risk analysis into the security requirements engineering process has been strongly suggested.

3 Background

3.1 The C&A Process

Compliance with regulatory requirements is mandatory if found applicable in the operational profile of the software system being certified. However, to consider the unique characteristics of each software system and its environment, C&A activities recommend a flexible risk-based strategy to come up with cost-effective security solutions [13]. Therefore, following the certification activities, the goal of accreditation activities is to agree upon an "acceptable level of risk" for authorizing system operation as shown in Fig. 2. The C&A process is not a one time effort, but it should be a commitment that lasts throughout the software system lifecycle, from inception through development, deployment and phase out [23].

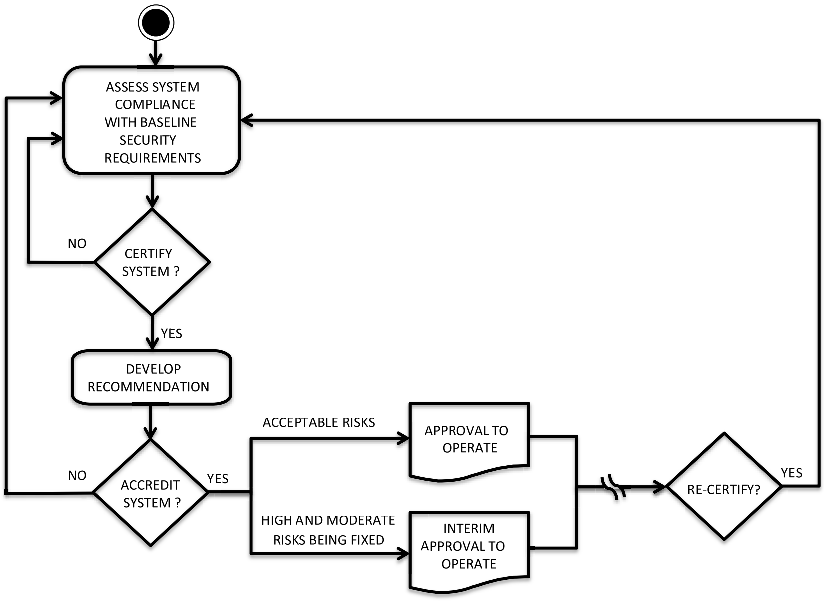

ASSESS SYSTEM COMPLIANCE WITH BASELINE SECURITY REQUIREMENTS
NO
CERTIFY SYSTEM ?
YES
DEVELOP RECOMMENDATION
NO
ACCREDIT SYSTEM ?
YES
ACCEPTABLE RISKS
APPROVAL TO OPERATE
HIGH AND MODERATE RISKS BEING FIXED
INTERIM APPROVAL TO OPERATE
RE-CERTIFY?
YES

Fig. 2 Certification and Accreditation Activities

DITSCAP [13] defines certification in the context of information systems as a comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. Following the certification activities, the accreditation statement is an approval to operate the information system in a particular security mode using a prescribed set of safeguards at an acceptable level of risk by a Designated Approving Authority (DAA). The key roles of the DITSCAP are the Program Manager, DAA, Certifier and the User Representative that tailor and scope the C&A efforts to the particular mission, environment, system architecture, threats, funding and schedule of the system through negotiations.

The DITSCAP requires that a "system" should be defined and agreed upon by the key roles, which is documented as a System Security Authorization Agreement (SSAA). DITSCAP follows a single document approach and records all artifacts produced through C&A activities into the SSAA. The SSAA is especially important because it is used throughout the entire DITSCAP to guide actions, document decisions, specify IA requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security [13]. The SSAA records the outcome of tasks and activities in each phase of the DITSCAP, which includes the metrics considered for the procurement of certification status.

3.2 Modeling C&A Requirements

C&A requirements specified at different levels of an organizational or governance hierarchy reflects the level of abstraction at which stakeholders perceive and understand security risks. The natural language specification of C&A requirements provide a rich context and rationale for the development of metrics and measures that are suitable to understand and communicate risk in a socio-technical environment. However, natural language C&A requirements have little or no structural regularity in their specifications and are scattered across several documents. In addition, demonstrating risks based on the level of compliance with C&A requirements involves a process of aggregating diverse metrics and measures as security risks only emerge upon interactions among components working together in a large and complex system.

It is apparent that any effort to understand risk by leveraging a standard baseline of C&A requirements will require: 1) identifying the attributes that classify and categorize the requirements from dimensions relevant to understanding risk; and 2) promoting a common understanding among stakeholders about the requirements and their relationships to various risk components. With respect to the latter, Wasson [49] demonstrates that capturing various explications of concepts related to domain semantics helps to better manage the risk of miscommunication in requirements. Explication of obligations and rights from regulatory policies to clarify ambiguities is suggested by Travis et al. [3]. Robinson et al. [37] suggest requirements structuring and grouping for identifying conflicts. To address both of the above concerns, rather than relying on any single modeling philosophy, in our approach, we explicate each C&A requirement based on attributes that capture the goals, scenarios, viewpoints and other domain-specific concepts necessary for precisely establishing their semantics as well as understand possible security risks in a socio-technical environment.

However, for natural language C&A requirements, these attributes are often missing, ambiguous or dispersed across multiple documents, limiting the use of formal approaches to process them. To address these issues, we have identified several heuristics that help in capturing the attributes of C&A requirements present sparsely in regulatory documents [27]. Specifically, guided by the Ontology-based

ACTive Requirements Engineering (Onto-ActRE) framework [28], we harness the expressiveness of ontologies to classify and categorize C&A requirements from the following dimensions: 1) a Requirements Domain Model (RDM) 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 DITSCAP by processing approximately 800 pages of regulatory documents (a representative set of DITSCAP related documents). The resulting DITSCAP PDO includes 604 domain concepts that help to understand 533 C&A requirements. Although, details about building the PDO are described in our prior publications [27] [29] [28]; here we briefly elaborate on the process of analyzing a DITSCAP requirement to identify relevant risk components, which is relevant to the scope of this chapter.

3.2.1 C&A Requirements and Risk Components

To support an overall risk-based strategy, for each C&A requirement we explicate relevant risk components. These are the threats to and vulnerabilities of the assets to be protected, and countermeasures that can mitigate or reduce the vulnerabilities to acceptable levels. 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 [9]. The resulting model, as shown in Fig. 3, explains the relationships between security requirements and risk components.

Based on the model in Fig. 3, for each C&A requirement, a domain expert identifies the relevant risk components and maps them to concepts in the domain-specific taxonomies of threats, assets, vulnerabilities, and countermeasures modeled in the PDO. Processing a C&A requirement description involves heuristics based on domain expertise, keyword analysis, regulatory document exploration, hierarchical browsing of concepts and navigating their relationships in the PDO. Fig. 4 shows the explication of multi-dimensional domain concepts for the DITSCAP "Boundary Defense" requirement [14].

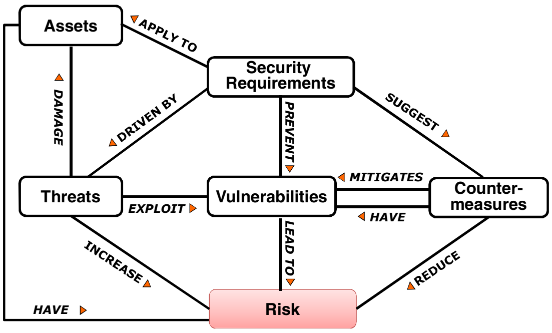


Fig. 3 Model of Relationships among Security Requirements and Risk Components

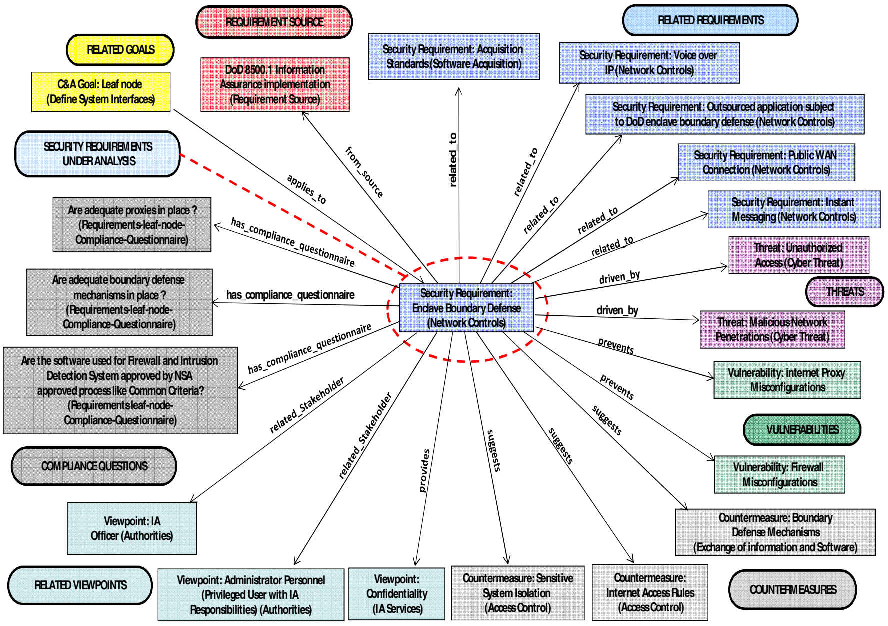
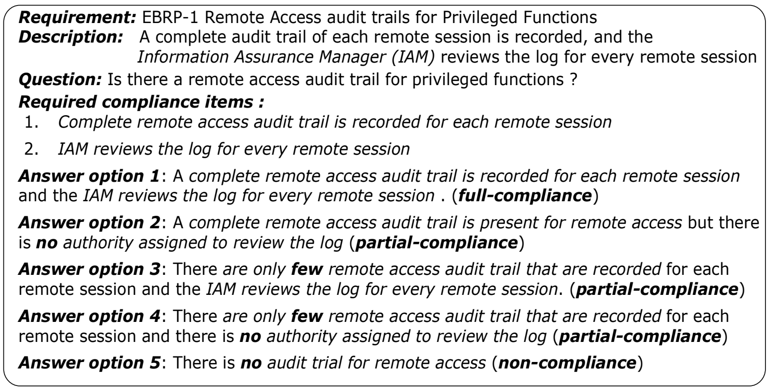

REQUIREMENT SOURCE
RELATED REQUIREMENTS
RELATED GOALS
C&A Goal: Leaf node (Define System Interfaces)
DoD 8500.1 Information Assurance implementation (Requirement Source)
Security Requirement: Acquisition Standards (Software Acquisition)
Security Requirement: Voice over IP (Network Controls)
Security Requirement: Outsourced application subject to DoD enclave boundary defense (Network Controls)
SECURITY REQUIREMENTS UNDER ANALYSIS
Security Requirement: Public WAN Connection (Network Controls)
Security Requirement: Instant Messaging (Network Controls)
applies_to
from_source
related_to
related_to
related_to
related_to
related_to
Are adequate proxies in place ? (Requirements-leaf-node-Compliance-Questionnaire)
has_compliance_questionnaire
Threat: Unauthorized Access (Cyber Threat)
driven_by
THREATS
Are adequate boundary defense mechanisms in place ? (Requirements-leaf-node-Compliance-Questionnaire)
has_compliance_questionnaire
Security Requirement: Enclave Boundary Defense (Network Controls)
driven_by
Threat: Malicious Network Penetrations (Cyber Threat)
Are the software used for Firewall and Intrusion Detection System approved by NSA approved process like Common Criteria? (Requirements leaf-node-Compliance-Questionnaire)
has_compliance_questionnaire
prevents
Vulnerability: internet Proxy Misconfigurations
prevents
related_Stakeholder
suggests
related_Stakeholder
VULNERABILITIES
COMPLIANCE QUESTIONS
provides
suggests
suggests
Vulnerability: Firewall Misconfigurations
Viewpoint: IA Officer (Authorities)
Countermeasure: Boundary Defense Mechanisms (Exchange of information and Software)
RELATED VIEWPOINTS
Viewpoint: Administrator Personnel (Privileged User with IA Responsibilities) (Authorities)
Viewpoint: Confidentiality (IA Services)
Countermeasure: Sensitive System Isolation (Access Control)
Countermeasure: Internet Access Rules (Access Control)
COUNTERMEASURES

Fig. 4 Analyzing a DITSCAP Requirement

Support for object-oriented ontological domain modeling in the Onto-ActRE framework is provided by the GENeric Object Model (GenOM) [32] toolkit. GenOM inherits the theoretical foundation of the frame representation and is compatible with the OKBC specification [7].

3.2.2 Information Gathering during C&A

C&A activities require collecting supporting evidences from the target system to determine the applicability as well as assess the level of compliance of C&A requirements. To conduct these information gathering activities, the PDO development involves the creation of two types of questionnaires for systematically capturing evidences that justify decision making activities based on objective and repeatable criteria. The first questionnaire set, called the *requirements applicability questionnaire*, captures the characteristics and constraints relevant to a software system in its operational environment and maps them to the characteristics/constraints of the security requirements categories in the Requirements Domain Model (RDM) of the PDO to determine their applicability. The requirements applicability questionnaires are hierarchically organized to prune the applicable requirements space based on the mappings of their member questions and corresponding answer options to the attributes of security requirements in the RDM.



Requirement: EBRP-1 Remote Access audit trails for Privileged Functions
Description: A complete audit trail of each remote session is recorded, and the *Information Assurance Manager (IAM)* reviews the log for every remote session
Question: Is there a remote access audit trail for privileged functions ?
Required compliance items :

1. *Complete remote access audit trail is recorded for each remote session*
2. *IAM reviews the log for every remote session*

Answer option 1: A *complete remote access audit trail is recorded for each remote session* and the *IAM reviews the log for every remote session* . (***full-compliance***)

Answer option 2: A *complete remote access audit trail is present for remote access* but there is ***no*** *authority assigned to review the log* (***partial-compliance***)

Answer option 3: There *are only* ***few*** *remote access audit trail that are recorded* for each remote session and the *IAM reviews the log for every remote session.* (***partial-compliance***)

Answer option 4: There *are only* ***few*** *remote access audit trail that are recorded* for each remote session and there is ***no*** *authority assigned to review the log* (***partial-compliance***)

Answer option 5: There is ***no*** *audit trial for remote access* (***non-compliance***)

Fig. 5 An Example Compliance Question and Answer Options

A second questionnaire set, called the *requirements compliance questionnaire*, establishes well-defined criteria to determine the compliance levels of each security requirement. For each C&A requirement the PDO development involves the identification of structured compliance criteria by a domain expert who has many years of experience in the field of performing C&A. Each compliance question has corresponding pre-defined answer options as ordered levels of compliance prepared from conjunction of the identified compliance criteria. The selected answer options can provide qualitative values (for requirements that cannot be evaluated based on a numerical scale are assigned to three qualitative compliance levels of full-compliance, partial-compliance or non-compliance, for example consider the requirement shown in Fig. 5) or quantitative values (typically numerical or Boolean values); however, both are normalized using appropriate weights to support uniform interpretation and evaluation of compliance levels in the application domain. Responses to the questions are gathered from various sources such as users, operating manuals, plans, architecture diagrams, or through automated network-based information discovery toolkits.

4 Ontology-Driven Metric Development

4.1 Multi-dimensional Link Analysis

Traceability within the PDO is essential to building cohesion among artifacts that may utilize diverse semantics or become available in different lifecycle stages of software development but are essential to understand emergent security risks. In other words, individual artifacts become valuable knowledge when they establish ‘links’ with each other from various aspects/dimensions based on the given problem frame [31]. Driven by this philosophy, within the PDO, we introduce Multi-Dimensional Link Analysis (MDLA) as a methodological support for developing metrics and measures. The complementary conceptual notions that guide the construction of the PDO allow MDLA to be triggered using domain concepts from multiple dimensions and at different levels of abstractions, while generating traceability among the developed metrics and measures based on designated ontological constructs. Through MDLA we seek to promote the assurance of a comprehensive coverage of the problem domain by actively assisting certification analysts in the process of discovering missing, conflicting, and interdependent pieces of evidence that help to understand risk.

With regards to the tasks and activities of the C&A process, MDLA provides an 'active' environment where the evidence gathered through the questionnaires as well as the interdependencies among the models in the PDO collectively help to produce metrics that have strong alignment and traceability with real world goals/objectives. In Table 1, we summarize the metrics derived from the different conceptual notions (Goals, Scenarios, Viewpoints and Domain-specific Concepts) that also guide the construction of the PDO. These metrics portray the multifaceted overlaps among socio-technical concepts that underlie the tasks, activities and stakeholders of the C&A process. Table 1 outlines the metrics resulting from the PDO and the corresponding execution of the C&A process from the following dimensions: 1) The conceptual modeling philosophy that drives metric development in a socio-technical environment; 2) The examined system artifact; 3) The structured representation of the selected artifact using ontological and knowledge engineering techniques; 4) The sources of information that are typically informal in nature and specified in natural language; 5) The C&A process roles that are involved in the production or consumption of the metrics; 6) The metrics developed based on the conceptual modeling philosophies, evidence from the system being certified, and the associated properties of designated ontological constructs; and 7) Derived metrics generated based on inferences from the preliminary metrics.

4.2 Ontology-Guided Risk Analysis

The metrics developed in the previous section are designed to facilitate the C&A process execution and understand the impact that security risks can have on real world business/mission. Building upon these metrics, it is necessary develop metrics that help to understand the security risks that only emerge upon interactions among various components working together in a system context. As a result, metrics that consider the cascading effects of a failure among interdependent security constraints working together in the operational context of the software system are required.

From a C&A process perspective rather than relying on the compliance assessment of each requirement individually, exploring 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 understand the possible risks due to non-compliance. We present a step-wise methodology in [16] for discovering and understanding the multi-dimensional 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 [16], here we briefly discuss the characteristics of the resulting visual risk assessment artifacts based on Formal Concept Analysis (FCA) [18]. Brief introduction to FCA can also be found in [16].

Table 1 Ontology-driven Metrics Development to facilitate the C&A Process

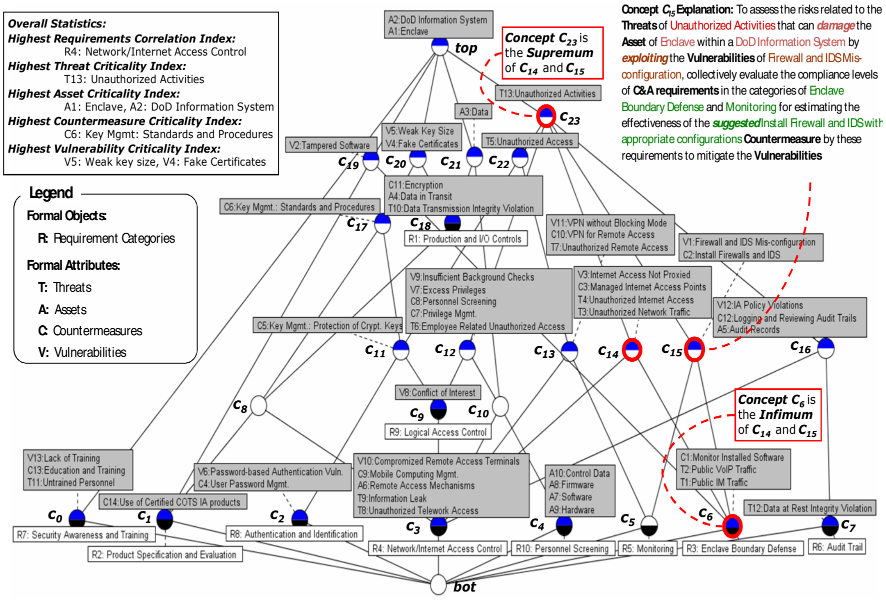
Category	Artifact	Representation	Source	Roles	Metrics	Derived Metrics
Goals	C&A process, tasks and activities	Hierarchical organization of process tasks with non-hierarchical interdependencies in the PDO	C&A Process documentation	DAA, Project manager, User representative	• Certification progress • Task/Activity requirements coverage • Relative interdependency of Tasks/Activities • Level of Task/Activity abstraction	• Process complexity • Task/Activity similarity • Documentation change impact • C&A process tool support configuration effort
Requirements	C&A requirements	Hierarchical organization of requirements types in the domain with non-hierarchical interdependencies in the PDO	Laws and policies, C&A requirements documents, General best practices, Site or agency specific documents and procedures	DAA, Project manager, Certifiers	• Security constraints coverage • Degree of requirements interdependencies • Level of abstraction of the requirements	• Security requirements complexity • Requirements similarity/proximity
Usage/Environment **Scenarios:** Applicability	C&A requirements	Hierarchical arrangement of questions based on a laddering mechanism to prune the requirements space	Domain expertise, C&A requirements documents, General best practices	Certifiers, User representatives	• Number of applicable security C&A requirements • Regulatory document coverage	• C&A effort estimation • Mission, system and information criticality
Usage/Environment **Scenarios:** Compliance	C&A requirements	Conjunction of IA metrics and measures from multiple dimensions organized into distinct compliance levels for each requirement, Sharing of evidence among requirements	Domain Expertise, C&A requirements documents, General best practices, Automated information gathering agents	DAA, Certifiers	• Requirements compliance level • Compliance evidence based requirements interdependency • Evidence collection progress • Technically oriented IA Metrics	• Compliance at different levels of abstraction of requirements • Compliance evidence driven impact analysis (FCA)
Viewpoints	System stakeholders and responsibilities, Security properties	Hierarchical arrangement of stakeholders and security expectations with non-hierarchical interdependencies in the PDO	C&A requirements documents and responsibility descriptions, Domain expertise	Certifiers	• Requirements coverage of a viewpoint • Amount of viewpoint intersections/ overlaps/ conflicts	• Level of responsibility satisfaction • Stakeholder criticality • Level of satisfaction of security expectations
Domain Specific Concepts: Risk Components	Threats, Assets, Countermeasures, Vulnerabilities	Hierarchical arrangement of each risk component with non-hierarchical interdependencies in the PDO	Laws and policies, C&A requirements documents, General best practices, Site or agency specific documents and procedures	DAA, Certifiers, User representative	• Requirements coverage of risk components • Degree of Risk component interdependencies • Level of abstraction of the risk components	• Risk mitigation level • Risk criticality
Ontological Constructs	All Domain Concepts	Generic ontological modeling constructs including objects, properties, features, object instances, features instances and rules	Laws and policies, C&A requirements documents, General best practices, Site or agency specific documents and procedures, and Domain expertise	All Roles	• Number of modeling constructs • Fan-in and Fan-out • Level of participation in problem solving	• Domain complexity • Concept similarity • Concept proximity • Propagative impact of non-compliance

The notion of risk being contextually subjective, we embed its assessment in the operational scenarios of the target system, whose selection is driven by the goals of the C&A process. For each scenario, we build an analysis pool as an exhaustive collection of C&A requirements that collectively constrain target system behavior within that scenario. A stepwise process of selecting the C&A requirements to be included in an analysis pool; and then, their abstraction to requirement categories (representative of security constraints) modeled in the PDO is required to build a formal context. Mathematically, a 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 Fig. 6 (Reproduced from [16]). 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).

4.2.1 Necessity and Sufficiency Metrics

A *formal concept* in Fig. 6 connects compliance to risk based on C&A requirement categories as its extent (reality) and risk components as its intent (human thinking/semantics). Such traceability is missing entirely in current methodologies for assessing risk. Mathematically, a *formal concept* establishes the "necessity and sufficiency" of a set of requirement categories to understand corresponding risks in a given operational scenario. For ease of understanding these characteristics, the natural language explanations of a *formal concept* is automatically generated by interpreting its intent, extent, and their relationships based on the requirements and risk model in Fig. 3 as well as the PDO. An example explanation of the node "C_{15}" is shown in Fig 6.


Overall Statistics:
Highest Requirements Correlation Index: R4: Network/Internet Access Control
Highest Threat Criticality Index: T13: Unauthorized Activities
Highest Asset Criticality Index: A1: Enclave, A2: DoD Information System
Highest Countermeasure Criticality Index: C6: Key Mgmt: Standards and Procedures
Highest Vulnerability Criticality Index: V5: Weak key size, V4: Fake Certificates

Concept C_{15} Explanation: To assess the risks related to the **Threats** of Unauthorized Activities that can *damage* the **Asset** of Enclave within a DoD Information System by *exploiting* the **Vulnerabilities** of Firewall and IDS Mis-configuration, collectively evaluate the compliance levels of **C&A requirements** in the categories of Enclave Boundary Defense and Monitoring for estimating the effectiveness of the *suggested* Install Firewall and IDS with appropriate configurations **Countermeasure** by these requirements to mitigate the **Vulnerabilities**

Concept C_{23} is the ***Supremum*** of C_{14} and C_{15}

Concept C_6 is the ***Infimum*** of C_{14} and C_{15}

Legend
Formal Objects:
R: Requirement Categories
Formal Attributes:
T: Threats
A: Assets
C: Countermeasures
V: Vulnerabilities
A2:DoD Information System
A1:Enclave
top
T13:Unauthorized Activities
A3:Data
c23
V2:Tampered Software
V5:Weak Key Size
V4:Fake Certificates
T5:Unauthorized Access
c19
c20
c21
c22
C11:Encryption
A4:Data in Transit
T10:Data Transmission Integrity Violation
C6:Key Mgmt.: Standards and Procedures
c17
c18
R1: Production and I/O Controls
V11:VPN without Blocking Mode
C10:VPN for Remote Access
T7:Unauthorized Remote Access
V1:Firewall and IDS Mis-configuration
C2:Install Firewalls and IDS
V9:Insufficient Background Checks
V7:Excess Privileges
C8:Personnel Screening
C7:Privilege Mgmt.
T6:Employee Related Unauthorized Access
V3:Internet Access Not Proxied
C3:Managed Internet Access Points
T4:Unauthorized Internet Access
T3:Unauthorized Network Traffic
V12:IA Policy Violations
C12:Logging and Reviewing Audit Trails
A5:Audit Records
C5:Key Mgmt.: Protection of Crypt. Keys
c11
c12
c13
c14
c15
c16
V8:Conflict of Interest
c8
c9
c10
R9: Logical Access Control
V13:Lack of Training
C13:Education and Training
T11:Untrained Personnel
V6:Password-based Authentication Vuln.
C4:User Password Mgmt.
V10:Compromized Remote Access Terminals
C9:Mobile Computing Mgmt.
A6:Remote Access Mechanisms
T9:Information Leak
T8:Unauthorized Telework Access
A10:Control Data
A8:Firmware
A7:Software
A9:Hardware
C1:Monitor Installed Software
T2:Public VoIP Traffic
T1:Public IM Traffic
C14:Use of Certified COTS IA products
T12:Data at Rest Integrity Violation
c0
c1
c2
c3
c4
c5
c6
c7
R7: Security Awareness and Training
R2: Product Specification and Evaluation
R8: Authentication and Identification
R4: Network/Internet Access Control
R10: Personnel Screening
R5: Monitoring
R3: Enclave Boundary Defense
R6: Audit Trail
bot

Fig. 6 An Example Concept Lattice for Remote Access Operational Scenario [16]

4.2.2 Propagative Impact and Prioritization Metrics

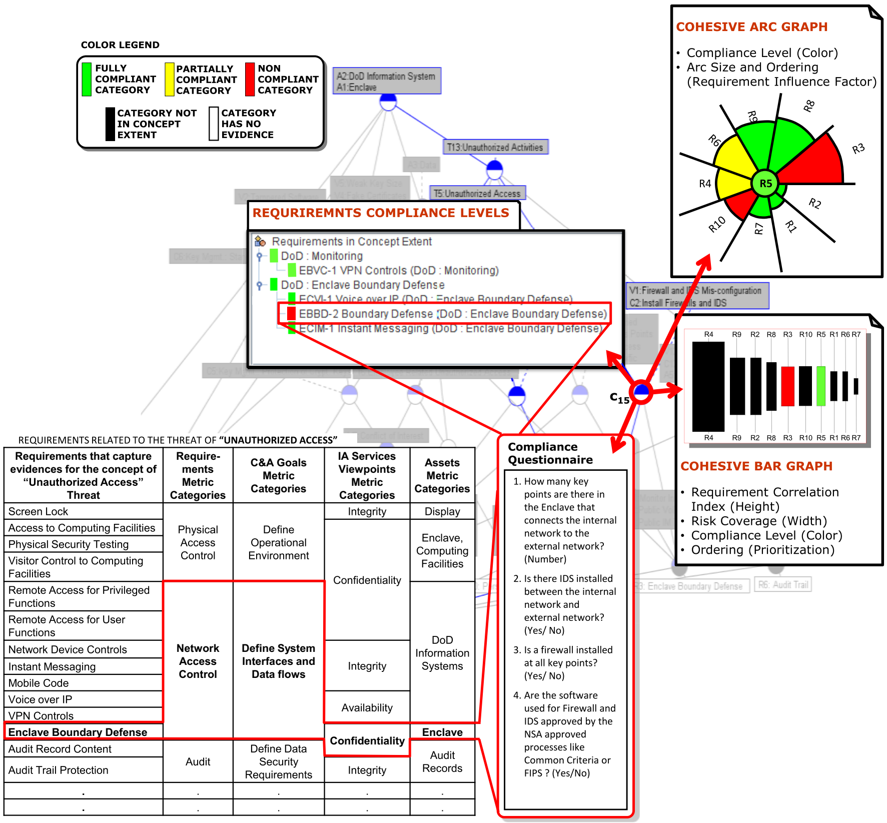
The representation of PDO combined with the algebraic operations upon *formal concepts* help produce well-defined metrics and measures to understand risks due to cascading effects of a failure/non-compliance in one or more security constraints. The first set of metrics convey the range of possible risks due to a simultaneous failure in multiple security constraints by identifying the 1) *Risk upper bound*; and 2) *Risk lower bound*, in terms of maximum and minimum number of security constraints that can be potentially bypassed by an attacker, respectively. These metrics correspond to computing the supremum and infimum [18] of a set of formal concepts that are most specific to the selected requirements categories.

The second set of metrics help to prioritize among requirement categories and risk components. 3) *Correlation index* for a requirement category is used as an indicator of its potential for correlation with other requirement categories. 4) *Criticality index* for a risk component is used as an indicator for its dependency on the collective compliance in many requirement categories. These metrics are shown in Fig 6 for a hypothetical scenario. 5) *Requirements influence factor* is used as an indicator for the degree of influence a given requirement category will have on the effective implementation of other requirement categories in a given scenario. The metrics in this set are derived primarily from the structural characteristics of the concept lattice.

A metric for risk coverage is derived from the lattice generated implication rules among risk components. *6) Mathematical risk coverage* can be determined to be 100% if the requirement categories that support the validity of implications in the stem base are fully compliant. For any non-compliant requirement categories, a subset of implications in the stem base can be identified to compute the set of all implications that follow. Mathematical details about these metrics can be found in [16][17].

4.3 Visualization for Metric Consumption and Exploration

Complex software-intensive systems present a diverse, large and dynamic information space with several metrics and measures. Therefore, to augment the analytical capabilities for risk assessment, we have developed visual metaphors that can illustrate critical requirements and the potential risks due to cascading effects of their non-compliance on overall system behavior. The goal of such visual analytics [50] is to combine human intuition with mathematically derived visual metaphors to facilitate decision making in a large information space.


COLOR LEGEND
🟩 FULLY COMPLIANT CATEGORY
🟨 PARTIALLY COMPLIANT CATEGORY
🟥 NON COMPLIANT CATEGORY
■ CATEGORY NOT IN CONCEPT EXTENT
□ CATEGORY HAS NO EVIDENCE
A2:DoD Information System
A1:Enclave
T13:Unauthorized Activities
T5:Unauthorized Access
V1:Firewall and IDS Mis-configuration
C2:Install Firewalls and IDS
C15
COHESIVE ARC GRAPH
• Compliance Level (Color)
• Arc Size and Ordering (Requirement Influence Factor)
R9
R8
R6
R3
R4
R5
R2
R10
R7
R1
R4 R9 R2 R8 R3 R10 R5 R1 R6 R7
COHESIVE BAR GRAPH
• Requirement Correlation Index (Height)
• Risk Coverage (Width)
• Compliance Level (Color)
• Ordering (Prioritization)

REQURIREMNTS COMPLIANCE LEVELS

Requirements in Concept Extent
- 🟩 DoD : Monitoring
  - 🟩 EBVC-1 VPN Controls (DoD : Monitoring)
- 🟩 DoD : Enclave Boundary Defense
  - 🟩 ECVI-1 Voice over IP (DoD : Enclave Boundary Defense)
  - 🟥 EBBD-2 Boundary Defense (DoD : Enclave Boundary Defense)
  - 🟩 ECIM-1 Instant Messaging (DoD : Enclave Boundary Defense)

REQUIREMENTS RELATED TO THE THREAT OF **"UNAUTHORIZED ACCESS"**

Requirements that capture evidences for the concept of "Unauthorized Access" Threat	Require-ments Metric Categories	C&A Goals Metric Categories	IA Services Viewpoints Metric Categories	Assets Metric Categories
Screen Lock	Physical Access Control	Define Operational Environment	Integrity	Display
Access to Computing Facilities			Confidentiality	Enclave, Computing Facilities
Physical Security Testing				
Visitor Control to Computing Facilities				
Remote Access for Privileged Functions	**Network Access Control**	**Define System Interfaces and Data flows**		DoD Information Systems
Remote Access for User Functions				
Network Device Controls			Integrity	
Instant Messaging				
Mobile Code				
Voice over IP			Availability	
VPN Controls				
Enclave Boundary Defense			**Confidentiality**	**Enclave**
Audit Record Content	Audit	Define Data Security Requirements		Audit Records
Audit Trail Protection			Integrity	
.	.	.	.	.
.	.	.	.	.

Compliance Questionnaire

1. How many key points are there in the Enclave that connects the internal network to the external network? (Number)
2. Is there IDS installed between the internal network and external network? (Yes/ No)
3. Is a firewall installed at all key points? (Yes/ No)
4. Are the software used for Firewall and IDS approved by the NSA approved processes like Common Criteria or FIPS ? (Yes/No)

Fig. 7 Visual Metaphors for Communicating and Exploring Metrics with respect to a *Formal Concept*

In Fig. 7 the visual metaphors: 1) *Cohesive bar graph*; and 2) *Cohesive arc graph* [17], convey metrics derived from the concept lattice, metrics gathered from requirements compliance questionnaires, and semantics derived from the PDO. Each *formal concept* provides a structured and well-understood context to use the metrics available through our methodology for understanding possible risks. In Fig. 7 the cohesive bar graph readily conveys the necessity and sufficiency of requirement categories R3 and R5 to address risk components in the intent of the *formal concept* C_{15}. To further complement this understanding, the cohesive arc graph conveys that the requirement R5 and R3 have relatively significant influence on the effective implementation of each other in the given sceanrio.

In addition to the abstract visual metaphors, the PDO provides an integrated environment where the evidence gathered in the form of IA metrics and measures from the solution space can be understood in the context of metrics resulting from MDLA in the conceptual problem space. In Fig. 7, the impact of non-compliance in the "Enclave boundary defense" requirement can be understood based on the IA metrics available as evidence from its compliance questionnaire. This evidence can also be traced back to the multiple dimensions in the PDO and related metrics (Table 1). This multi-dimensional traceability provides the ability to explore and study metrics that are grounded in the original abstractions used to understand and characterize the problem space.

Table 2 Ontology driven Metric Development for Understanding Emergent Security Risks

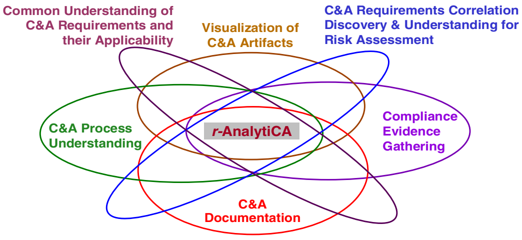
Category	Artifact	Representation	Source	Roles	Metrics	Derived Metrics
Operational Scenarios	System Use and Function	Analysis Pool for Risk Assessment: Exhaustive collection of C&A requirements applicable in a operational scenario of the target system	System Use Cases, Misuse cases, User manual,	Certifiers, Program Mangers, User represen-tative	• C&A Requirements diversity for risks assessment • Scenario Similarity • C&A Process/Goal Coverage	• Risk Assessment Scope • Justifiability of Requirements selection for Risk Assessment • Complexity of the risk assessment effort • Level of rigor in risk assessment
Require-ments Correlations	Requirements and Risk Components	A complete lattice of all potential interdependencies among requirements based on related risk components. Formal Concept Analysis	PDO, Risk Assessment Goals and Scenario, Analysis Pool	Certifiers, DAA	• Requirement Necessity for addressing Risk components • Requirements Sufficiency for addressing Risks Components • Requirements Overlap • Risk Coverage of Requirements	• Risk Upper and Lower bounds of non-compliance • Requirements Correlation Index • Risk Component Criticality Index • Requirement Influence on the effective implementation of other requirements • Non-compliance impact
Visual Metaphors	Requirements and Risk Components	Visual representations of qualitative and quantitative metrics	PDO, Risk Assessment Goals and Scenario, Analysis Pool, Requirements Compliance	All stake-holders	• Requirements Prioritization • Risk Component Prioritization • Non-compliance impact	• Non-compliance Sensitivity • Visual perceptions of abnormal and normal behavior

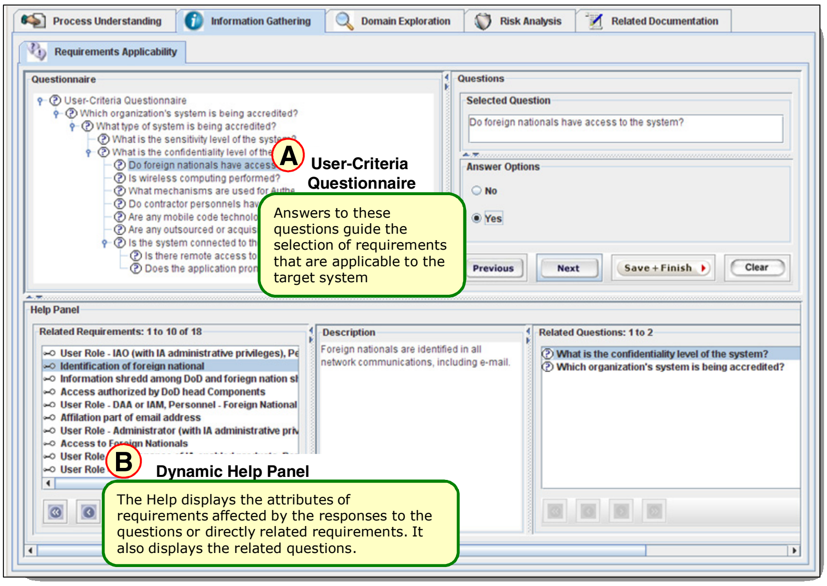
As a continuation of Table1, Table 2 summarizes the metrics developed to understand the security risks that only emerge upon interactions among various components working together in a system context.

5 r-AnalytiCA Workbench

Our approach has been manifested in a C&A tool suite: The r-AnalytiCA (Requirements Analytics for Certification & Accreditation) Workbench [26]. The r-AnalytiCA workbench leverages the expressiveness of the PDO to address the complexities associated with C&A tasks and activities. Its purpose is to enable various requirements analytics for providing meaningful insights to a certification analyst into the evidence gathered during the C&A process. Fig. 8 shows the

Fig. 8 Application Areas of r-AnalytiCA Workbench


Common Understanding of C&A Requirements and their Applicability
Visualization of C&A Artifacts
C&A Requirements Correlation Discovery & Understanding for Risk Assessment
C&A Process Understanding
r-AnalytiCA
Compliance Evidence Gathering
C&A Documentation



Questionnaire

- User-Criteria Questionnaire
  - Which organization's system is being accredited?
    - What type of system is being accredited?
      - What is the sensitivity level of the system?
      - What is the confidentiality level of the
        - Do foreign nationals have access
        - Is wireless computing performed?
        - What mechanisms are used for Authe
        - Do contractor personnels hav
        - Are any mobile code technolo
        - Are any outsourced or acquis
        - Is the system connected to th
          - Is there remote access to
          - Does the application pron

Questions

Selected Question: Do foreign nationals have access to the system?

Answer Options: ○ No ● Yes

A **User-Criteria Questionnaire**

Answers to these questions guide the selection of requirements that are applicable to the target system

Help Panel

Related Requirements: 1 to 10 of 18

- User Role - IAO (with IA administrative privileges), Pe
- Identification of foreign national
- Information shredd among DoD and foriegn nation sl
- Access authorized by DoD head Components
- User Role - DAA or IAM, Personnel - Foreign National
- Affilation part of email address
- User Role - Administrator (with IA administrative priv
- Access to Foreign Nationals
- User Role
- User Role

Description: Foreign nationals are identified in all network communications, including e-mail.

Related Questions: 1 to 2

- What is the confidentiality level of the system?
- Which organization's system is being accredited?

B **Dynamic Help Panel**

The Help displays the attributes of requirements affected by the responses to the questions or directly related requirements. It also displays the related questions.

Fig. 9 Requirements Applicability Questionnaire Interface in r-AnalytiCA

currently supported application areas of the r-AnalytiCA workbench. The key strength of r-AnalytiCA is to be able to create synergy among its application areas for producing insightful C&A artifacts.

From a methodological aspect, the r-AnalytiCA first supports information (evidence) gathering activities and later supports analytical activities such as risk assessment upon the collected evidences. To bootstrap the C&A process, rather than selecting regulations (as in other C&A tools), the workbench presents the requirements applicability questionnaires through a wizard-based interface as shown in Fig 9. The context of each question (Fig. 9 Label A) is explicated based on its related requirements, requirements properties and related questions (Fig. 9 Label B) in the PDO. After answering the applicability questionnaire, stakeholders can browse the selected requirements and related concepts in the PDO as well as record evidence using interfaces that present the requirements compliance questionnaire.

Following the information gathering activities, the risk analysis activities are initated in the workbench using interfaces that support goal driven scenario composition (Fig. 10 Label 1). To form an analysis pool for each scenario the analyst can search for relevant C&A requirements in the PDO based on 1) keywords (Fig. 10 Label 2); 2) focused hierarchical browsing of requirements categories (Fig. 10

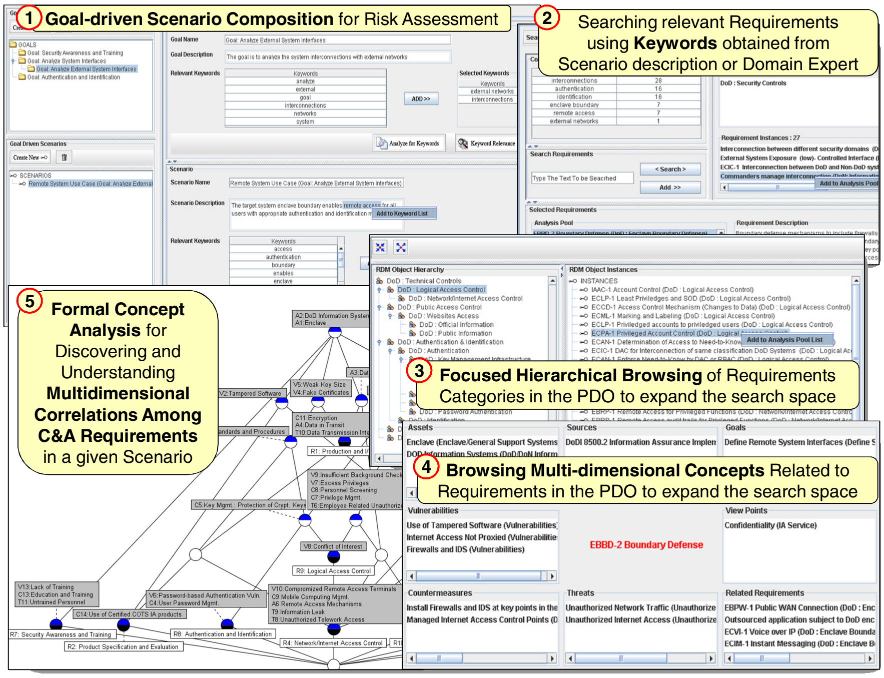
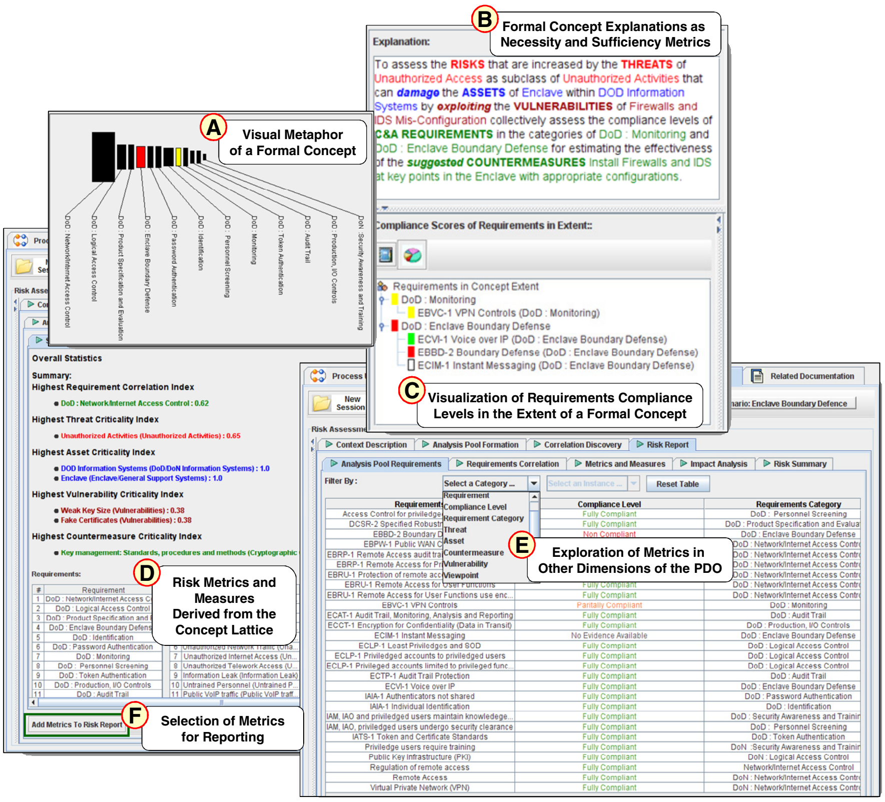

1 Goal-driven Scenario Composition for Risk Assessment
2 Searching relevant Requirements using Keywords obtained from Scenario description or Domain Expert
3 Focused Hierarchical Browsing of Requirements Categories in the PDO to expand the search space
4 Browsing Multi-dimensional Concepts Related to Requirements in the PDO to expand the search space
5 Formal Concept Analysis for Discovering and Understanding Multidimensional Correlations Among C&A Requirements in a given Scenario
EBBD-2 Boundary Defense

Fig. 10 Risk Assessment Interfaces in r-AnalytiCA


A
Visual Metaphor of a Formal Concept
DoD : Network/Internet Access Control
DoD : Logical Access Control
DoD : Product Specification and Evaluation
DoD : Enclave Boundary Defense
DoD : Password Authentication
DoD : Identification
DoD : Personnel Screening
DoD : Monitoring
DoD : Token Authentication
DoD : Audit Trail
DoD : Production, I/O Controls
DoN :Security Awareness and Training
B
Formal Concept Explanations as Necessity and Sufficiency Metrics
C
Visualization of Requirements Compliance Levels in the Extent of a Formal Concept
D
Risk Metrics and Measures Derived from the Concept Lattice
E
Exploration of Metrics in Other Dimensions of the PDO
F
Selection of Metrics for Reporting
Process
New Session
Risk Assessment
Related Documentation
ario: Enclave Boundary Defence
Context Description
Analysis Pool Formation
Correlation Discovery
Risk Report
Analysis Pool Requirements
Requirements Correlation
Metrics and Measures
Impact Analysis
Risk Summary
Add Metrics To Risk Report

Explanation:

To assess the **RISKS** that are increased by the **THREATS** of Unauthorized Access as subclass of Unauthorized Activities that can ***damage*** the **ASSETS** of Enclave within DOD Information Systems by ***exploiting*** the **VULNERABILITIES** of Firewalls and IDS Mis-Configuration collectively assess the compliance levels of **C&A REQUIREMENTS** in the categories of DoD : Monitoring and DoD : Enclave Boundary Defense for estimating the effectiveness of the ***suggested*** **COUNTERMEASURES** Install Firewalls and IDS at key points in the Enclave with appropriate configurations.

Compliance Scores of Requirements in Extent::

Requirements in Concept Extent
- 🟨 DoD : Monitoring
  - 🟨 EBVC-1 VPN Controls (DoD : Monitoring)
- 🟥 DoD : Enclave Boundary Defense
  - 🟩 ECVI-1 Voice over IP (DoD : Enclave Boundary Defense)
  - 🟥 EBBD-2 Boundary Defense (DoD : Enclave Boundary Defense)
  - □ ECIM-1 Instant Messaging (DoD : Enclave Boundary Defense)

Overall Statistics

Summary:

Highest Requirement Correlation Index
- DoD : Network/Internet Access Control : 0.62

Highest Threat Criticality Index
- Unauthorized Activities (Unauthorized Activities) : 0.65

Highest Asset Criticality Index
- DOD Information Systems (DoD/DoN Information Systems) : 1.0
- Enclave (Enclave/General Support Systems) : 1.0

Highest Vulnerability Criticality Index
- Weak Key Size (Vulnerabilities) : 0.38
- Fake Certificates (Vulnerabilities) : 0.38

Highest Countermeasure Criticality Index
- Key management: Standards, procedures and methods (Cryptographic

Requirements:

#	Requirement	#	
1	DoD : Network/Internet Access C		
2	DoD : Logical Access Control		
3	DoD : Product Specification and		
4	DoD : Enclave Boundary Defens		
5	DoD : Identification		
6	DoD : Password Authentication	6	Unauthorized Network Traffic (Una...
7	DoD : Monitoring	7	Unauthorized Internet Access (Un...
8	DoD : Personnel Screening	8	Unauthorized Telework Access (U...
9	DoD : Token Authentication	9	Information Leak (Information Leak)
10	DoD : Production, I/O Controls	10	Untrained Personnel (Untrained P...
11	DoD : Audit Trail	11	Public VoIP traffic (Public VoIP traff...

Filter By : Select a Category ... | Select an Instance ... | Reset Table

Requirement
Compliance Level
Requirement Category
Threat
Asset
Countermeasure
Vulnerability
Viewpoint

Requirements	Compliance Level	Requirements Category
Access Control for priviledge	Fully Compliant	DoD : Personnel Screening
DCSR-2 Specified Robustr	Fully Compliant	DoD : Product Specification and Evalua
EBBD-2 Boundary D	Non Compliant	DoD : Enclave Boundary Defense
EBPW-1 Public WAN C		DoD : Network/Internet Access Contr
EBRP-1 Remote Access audit tra		DoD : Network/Internet Access Contr
EBRP-1 Remote Access for Pr		DoD : Network/Internet Access Contr
EBRU-1 Protection of remote acc		DoD : Network/Internet Access Contr
EBRU-1 Remote Access for User Functions	Fully Compliant	DoD : Network/Internet Access Contr
EBRU-1 Remote Access for User Functions use enc...	Fully Compliant	DoD : Network/Internet Access Contr
EBVC-1 VPN Controls	Paritally Compliant	DoD : Monitoring
ECAT-1 Audit Trail, Monitoring, Analysis and Reporting	Fully Compliant	DoD : Audit Trail
ECCT-1 Encryption for Confidentiality (Data in Transit)	Fully Compliant	DoD : Production, I/O Controls
ECIM-1 Instant Messaging	No Evidence Available	DoD : Enclave Boundary Defense
ECLP-1 Least Priviledges and SOD	Fully Compliant	DoD : Logical Access Control
ECLP-1 Priviledged accounts to priviledged users	Fully Compliant	DoD : Logical Access Control
ECLP-1 Privileged accounts limited to privileged func...	Fully Compliant	DoD : Logical Access Control
ECTP-1 Audit Trail Protection	Fully Compliant	DoD : Audit Trail
ECVI-1 Voice over IP	Fully Compliant	DoD : Enclave Boundary Defense
IAIA-1 Authenticators not shared	Fully Compliant	DoD : Password Authentication
IAIA-1 Individual Identification	Fully Compliant	DoD : Identification
IAM, IAO and priviledged users maintain knowledege...	Fully Compliant	DoD : Security Awareness and Trainin
IAM, IAO, priviledged users undergo security clearance	Fully Compliant	DoD : Personnel Screening
IATS-1 Token and Certificate Standards	Fully Compliant	DoD : Token Authentication
Priviledge users require training	Fully Compliant	DoN :Security Awareness and Trainin
Public Key Infrastructure (PKI)	Fully Compliant	DoN : Logical Access Control
Regulation of remote access	Fully Compliant	Network/Internet Access Control
Remote Access	Fully Compliant	DoN : Network/Internet Access Contr
Virtual Private Network (VPN)	Fully Compliant	DoN : Network/Internet Access Contr

Fig. 11 Risk Metrics and Measures Reporting Interfaces in r-AnalytiCA

Label 3); and 3) browsing multi-dimensional concepts related to requirements (Fig. 10 Label 4). After this step, the requirements in the analysis pool are used to compute the FCA lattice (Fig.10 Label 5). Each formal concept in the FCA lattice helps to understand risk based on C&A requirements in its extent and risk components in its intent (Fig. 11, Label B).

With the availability of a FCA lattice, the workbench supports the creation of a comprehensive report through the selection of relevant metrics and measures to understand risk. Fig. 11 depicts several interfaces in the workbench that can be used to create a risk report by selectively including metrics and measures in a textual or visual format. Selective reporting focuses the examination of risk in a given scenario to only non-compliant requirements or certain risk components. In addition, specific "what-if" scenarios can be constructed that embed the analysis artifacts in context with real world events and actors.

The workbench architecture is easily tailorable to accommodate different C&A processes, quality regulations (e.g. security, safety, privacy, etc.), and organizational needs. A Process-Aspect Ontology [30] dynamically composes the services that expose the domain models in the PDO with user interface components in the workbench. Finally, all artifacts resulting from the workbench are aggregated based on the ontological definition of the standard C&A document template (For example, the SSAA outline [12] for DITSCAP).

6 Concluding Remarks and Future Work

Complex social phenomena plays a key role in the success of all modern computing technologies. Such interdependency demands a more precise definition of the metrics and measures used in their planning, development and evaluation. In this direction, our approach for combining the fundamental conceptual notions of requirements engineering in an ontological engineering framework is a novel approach with promising initial results for metric development. Through this process, metrics emerge naturally from a modeling effort to structure and understand the problem domain, rather than an after-thought. From this perspective we identify the following contributions. Firstly, we have outlined a comprehensive framework for eliciting, representing, and structuring problem domain concepts from several informal sources. This effort facilitates the development of metrics that are well-defined (formal) and closer to the real world goals, system operational scenarios, stakeholder viewpoints and application specific concepts such as risk assessment. In other words, we have demonstrated the development of rigorous (formal and justifiable) qualitative and quantitative metrics, and analyzing their inter/intra-dependencies driven by regulatory requirements (informal sources) applicable to an organization. The application of our framework in the context of the DITSCAP establishes its initial feasibility and illustrates several heuristics for ontological engineering from regulatory documents.

Secondly, we introduce MDLA for analytical analysis which promotes cohesion between metrics and measures expressed in different ways or obtained from different sources. It facilitates an ontology-driven approach to produce metrics for understanding risks, which may only emerge upon interaction among components in a system context. A novel contribution is the direct association of metrics for requirements compliance levels with risk components whose interactions may lead to risk. Such traceability is missing entirely in current methodologies for assessing risk during the C&A process.

Thirdly, our use of visualization to consume and explore complementary metrics offers the ability to maintain global as well as local awareness of problem domain concepts while making critical decisions. In a large problem domain, the use of FCA provides a bounded (local) context to examine and recall metrics that are relevant to understand risk in operational scenarios of the target system; while the traceability in the PDO allows the impact to be examined at a global scope. This approach allows an interactive selection of an appropriate level of abstraction to analyze or communicate metrics for a large and complex system.

Finally, our research contributions have been applied in the development of the r-AnalytiCA workbench. The purpose of the workbench is to provide programmatic support for building problem solving techniques by leveraging the strengths of ontology-based domain modeling and aggregation of metrics based on multiple requirements engineering philosophies. The workbench allows a traceable chain of analytical thoughts grounded in regulatory policies and requirements to be explicitly associated with software development artifacts.

As part of our ongoing and future work we have conducted several case study sessions with subject matter experts in the C&A and risk assessment domain to validate the claims made through our research. This validation effort will reflect upon the fitness of the available metrics and measures to address current shortcomings of the C&A process. In addition, expert feedback is being used to improve the usability of the r-AnalytiCA workbench and metric visualizations.

References

1. Aagedal, J.O., den Braber, F., Dimitrakos, T., Gran, B.A., Raptis, D., Stolen, K.: Model-based risk assessment to improve enterprise security. In: Proceedings of the 6th International Enterprise Distributed Object Computing Conference, pp. 51–62 (2002)
2. Basili, V.R., Rombach, H.D.: The TAME project: Towards improvement-oriented software environments. IEEE Transactions on Software Engineering 14(6), 758–773 (1988)
3. Breaux, T.D., Vail, M.W., Antón, A.I.: Towards Regulatory Compliance: Extracting Rights & Obligations to Align Requirements with Regulations. In: Proc. 14th Int'l Conf. on RE 2006, pp. 49–58 (2006)
4. Butler, S.A.: Security Attribute Evaluation Method: A Cost Benefit Approach. In: Proceedings of the 24th International Conference on Software Engineering, May 2002, pp. 232–240 (2002)
5. Butler, S.A., Shaw, M.: Incorporating Nontechnical Attributes in Multi-Attribute Analysis for Security. In: Proceedings of the Workshop on Economics-Driven Software Engineering Research (2002), `http://www-2.cs.cmu.edu/~shawnb/EDSERIV.pdf`
6. Carr, M.J., et al.: Taxonomy-Based Risk Identification. Tech. Report CMU/SEI-93-TR-6 ESC-TR-93-183 (1993)
7. Chaudhri, V.K., Farquhar, A., Fikes, R., Karp, P.D., Rice, J.P.: OKBC: a programmatic foundation for knowledge base interoperability. In: Proceedings of the 15th National/10th Conference on Artificial intelligence/innovative Applications of Artificial intelligence, pp. 600–607. AAAI, Menlo Park (1998)
8. Alberts, C., Dorofee, A.: Managing Information Security Risks: The OCTAVE$^{(SM)}$ Approach. Addison-Wesley Professional, Reading (2002)
9. Common Criteria, Part 1: Introduction and General Model, v2.3, ISO/IEC 15408 (August 2005)
10. Common Weakness Enumeration, `http://cve.mitre.org/cwe/`
11. Davis, T.: Federal Computer Security Report Card Grades. Press Release (2004)
12. DoD 8510.1-M: DITSCAP Application Manual (2000)
13. DoD Instruction 5200.40: DITSCAP (1997)
14. DoDI 8500.2: IA Implementation (February 2003)
15. Feather, M.S., Cornford, S.L.: Quantitative risk-based requirements reasoning. Requirements Engineering Journal 8(4), 248–265 (2003)
16. Gandhi, R.A., Lee, S.W.: Discovering and Understanding Multi-dimensional Correlations among Certification Requirements with application to Risk Assessment. In: Proceedings of the 15th IEEE International Requirements Engineering Conference (RE 07), Delhi, India, October 15-19, (2007)

17. Gandhi, R.A., Lee, S.W.: Visual Analytics for Requirements-driven Risk Assessment. In: The Proceedings of 2nd International Workshop on Requirements Engineering Visualization (REV 2007) at the 15th IEEE International Requirements Engineering Conference (RE 2007), Delhi, India, October 15-19 (2007)
18. Ganter, B., Wille, R.: Formal Concept Analysis. Springer, Heidelberg (1996)
19. Jackson, M.: The Meaning of Requirements, in Annals of Software Engineering, vol. 3, pp. 5–21. Baltzer Science Publication (1997)
20. Johansson, E., Johnson, P.: Assessment of Enterprise Information Security - Estimating the Credibility of the Results. In: Proceedings of the Symposium on Requirements Engineering for Information Security (SREIS 2005) in conjunction with the 13th IEEE International Requirements Engineering Conference (RE 2005), Paris, France, 8/29 – 9/2. IEEE Press, Los Alamitos (2005)
21. Juristo, N., Moreno, A.M.: Introductory paper: Reflections on Conceptual Modeling. Data & Knowledge Engineering 33(2), 103–117 (2000)
22. Kaplan, R.S., Norton, D.P.: The Balanced Scorecard: Translating Strategy into Action. Harvard Business School Press, Boston (1996)
23. Kimbell, J., Walrath, M.: Life Cycle Security and DITSCAP. IANewsletter 4(2) (Spring 2001), `http://iac.dtic.mil/iatac`
24. Kotonya, G., Sommerville, I.: Requirements engineering with viewpoints. Software Engineering Journal 11(1), 5–18 (1996)
25. Lee, S.W., Gandhi, R.A., Ahn, G.: Certification Process Artifacts Defined as Measurable Units for Software-intensive Systems Lifecycle. International Journal on Software Process: Improvement and Practice 12(2), 165–189 (2007)
26. Lee, S.W., Gandhi, R.A., Wagle, S.J., Murty, A.B.: r-AnalytiCA Workbench: Requirements Analytics for Certification & Accreditation. In: Proceedings of the IEEE 15th International Requirements Engineering Conference (RE 2007), Posters, Demos and Exhibits Session, Delhi, India, October 15-19 (2007)
27. Lee, S.W., Muthurajan, D., Gandhi, R.A., Yavagal, D., Ahn, G.: Building Decision Support Problem Domain Ontology from Security Requirements to Engineer Software-intensive Systems. International Journal on Software Engineering and Knowledge Engineering 16(6), 851–884 (2006)
28. Lee, S.W., Gandhi, R.A.: Ontology-based Active Requirements Engineering Framework. In: Proceedings of the 12th Asia-Pacific Software Engineering Conference (APSEC 2005), Taipei, Taiwan, December 15-17, 2005, pp. 481–490. IEEE Computer Society Press, Los Alamitos (2005)
29. Lee, S.W., Gandhi, R.A.: Requirements as Enablers for Software Assurance. CrossTalk: The Journal of Defense Software Engineering 19(12), 20–24 (2006)
30. Lee, S.W., Gandhi, R.A., Wagle, S.J.: Ontology-guided Service-oriented Architecture Composition to Support Complex and Evolving Process Definitions. To appear in the International Journal of Software Engineering and Knowledge Engineering(March 2008) (accepted July 14, 2008)
31. Lee, S.W., Rine, D.C.: Missing Requirements and Relationship Discovery through Proxy Viewpoints Model. Studia Informatica Universalis: International Journal on Informatics 3(3), 315–342 (2004)
32. Lee, S.W., Wagle, S., Gandhi, R.A.: GenOM/GenOM-DB Programmer's Guide. Version 3, Technical Report TR-NISE-07-04, Knowledge Intensive Software Engineering Research Group, Dept. of Software and Information Systems, UNC Charlotte (2007)
33. Lekkas, D., Spinellis, D.: Handling and Reporting Security Advisories: A Scorecard Approach. IEEE Security and Privacy Magazine 3(4), 32–41 (2005)

34. Mead, N.R., Hough, E., Stehney, T.: Security Quality Requirements Engineering (SQUARE) Methodology. Technical Report (CMU/SEI-2005-TR-009). Software Engineering Institute, Carnegie Mellon University, Pittsburgh (2005)
35. Moffett, J.D., Haley, C.B., Nuseibeh, B.A.: Core Security Requirements Artefacts. Technical Report 2004/23. Department of Computing, The Open University, Milton Keynes (June 2004)
36. Black, P.E.: SAMATE's contribution to Information Assurance. IAnewsletter 9(2) (Fall 2006), http://iac.dtic.mil/iatac
37. Robinson, W.N., Pawlowski, S.: Surfacing Root Requirements Interactions from Inquiry Cycle Requirements. In: Proc. 6th Int'l Conf. on RE, pp. 82–89 (1998)
38. Rolland, C., Prakash, N.: From conceptual modeling to requirements engineering. Annals of Software Engineering 10, 151–176 (2000)
39. SAMATE Reference Dataset, http://samate.nist.gov/SRD/
40. Sutcliffe, A.: Scenario-based requirements analysis. Requirements Engineering Journal 3(1), 48–65 (1998)
41. Swanson, M., Bartol, N., Sabato, J., Hash, J., Graffo, L.: Security Metrics Guide for Information Technology Systems. NIST Special Publication #800-55, Gaithersburg, MD, USA (2003)
42. Swanson, M., Bartol, N., Sabato, J., Hash, J., Graffo, L.: Security Metrics Guide for Information Technology Systems. In: NIST Special Publication #800-55, Revised as Performance Measurement Guide for Information Security, Gaithersburg, MD, USA (July 2008)
43. Swartout, W., Tate, A.: Ontologies. IEEE Intelligent Systems 14(1), 18–19 (1999)
44. Tsipenyuk, K., Chess, B., McGraw, G.: Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors. IEEE Security & Privacy Magazine 3(6), 81–84 (2005)
45. van Lamsweerde, A.: Goal-oriented requirements engineering: a guided tour. In: Proceedings of the fifth IEEE International Symposium on Requirements Engineering, August 2001, pp. 249–262 (2001)
46. Vaughn, R.B., Henning, R., Siraj, A.: Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy. In: Proceedings of the 36th Annual Hawaii International Conference on System Sciences, pp. 331–340 (2003)
47. Verdon, D., McGraw, G.: Risk Analysis in Software Design. IEEE Security & Privacy Magazine 2(4), 79–84 (2004)
48. Wang, H., Wang, C.: Taxonomy of Security Considerations and Software Quality. Communications of the ACM 46(6), 75–78 (2003)
49. Wasson, K.S.: A Case Study in Systematic Improvement of Language for Requirements. In: 14th Int'l RE Conf., pp. 6–15 (2006)
50. Wong, P.C., Thomas, J.: Visual Analytics. IEEE Computer Graphics and Applications 24(5), 20–21 (2004)