To appear in Proceedings of the 15th IEEE International Requirements Engineering Conference (RE 07), October 15-19, Delhi, India, 2007.

Discovering and Understanding Multi-dimensional Correlations among Certification Requirements with application to 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

In this paper we outline our approach to discover and understand multi-dimensional correlations among regulatory security certification requirements in the context of a complex software system. A thorough understanding of these correlations is necessary to assure that diverse constraints imposed by numerous certification requirements are adequate for collectively contributing to emergent security properties in a highly interconnected socio-technical environment. We elaborate on methodological support to discover an exhaustive set of applicable certification requirements in a given operational scenario of the target software system. We then describe techniques to systematically understand the multi-dimensional correlations among these requirements with application to security risk assessment. The case study of applying our approach to a regulatory certification process of The United States Department of Defense (DoD) is presented.

1. Introduction

The government, defense, and private sectors spend billions of dollars every year in securing software systems that support their critical businesses/missions. A large portion of this money is now allocated for Certification and Accreditation (C&A) activities because of the growing number of regulations and the dire consequences of not complying with them. A recent survey [16] – representing 1,300 global companies, government and non-profit agencies in 55 nations – suggests that compliance with regulations has taken the lead as the primary driver of security efforts in an organization, surpassing worms and viruses. However, various reports [9] [16] [44] [45] [37] indicate that the process of measuring compliance with security C&A requirements is often irregular and unreliable. As a result, C&A processes lack consistent and comparable results and fail to provide adequate information for authorizing officials to understand security risks and make informed decisions [44].

Security certification is a comprehensive evaluation of the technical and non-technical security features of a software system to establish the extent to which a particular design and implementation meets a set of specified security requirements [11]. Compliance with C&A requirements is mandatory if found applicable to the target software system in its operational profile.

Security C&A requirements are generally non-functional. In addition, regulatory requirements reflect the interests of multiple stakeholders in the organization at different levels of abstraction. As a result, numerous C&A security requirements are scattered across multiple regulatory documents without any regularity in their natural language specifications, or appropriate classification and categorization about the types of constraints they enforce on system behavior. For example, some requirements impose abstract constraints that cross-cut many aspects of system behavior, whereas other requirements mandate specific constraints, which are applicable only in a particular instance of system design and implementation. As a result, a great deal of subjectivity surrounds C&A requirements and the ensuing risk assessment to determine what constraints on software behavior are adequate and what level of resources should be expended upon them [45].

Security C&A approaches generally recommend a risk-based strategy to provide cost-effective security solutions in the context of the target system [11]. Towards this goal, natural language specifications of security C&A requirements are tailored to embed domain semantics related to understanding relevant security risks in the unique socio-technical environment of an organizational infrastructure. Application requirements and real use cases are also necessary to effectively assess security risks [13]. Therefore, justifiable secure software assurance requires demonstrating that all critical security risks have been assessed in the operational context of the target software system and reduced to an acceptable level. However, due to the nature of current software systems, as interconnected systems of systems operational within socio-technical environments, such assurances are difficult to make.

Security being an emergent property of the system as a whole; 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. Therefore, discovering and understanding the multi-dimensional correlations among the different classes of constraints imposed by an exhaustive set of C&A requirements found applicable in the operational context of a complex software system is important to uncover and assess all possible potential risks. In our research, we leverage the semantics of each C&A requirement explicated by relationships with relevant domain concepts in a Problem Domain Ontology (PDO) built from C&A regulatory documents [27] [29]. We discuss methodological steps to discover applicable C&A requirements and understand the correlations among them from the perspective of risk assessment for a particular operational scenario of the target system. Correlations among C&A requirements that represent different classes of security constraints are analyzed by applying the algebraic model of Formal Concept Analysis (FCA) [18] along with the domain semantics learned from the PDO. The case study of applying our approach to The United States DoD Information Technology Security Certification and Accreditation Process (DITSCAP) [11] is presented.

Organization of the paper is as follows. Section 2 presents the related work and the relevant aspects of our prior research. Section 3 outlines methodological steps in our approach and the associated techniques. Section 4 discusses the use of artifacts resulting from our approach towards C&A documentation. Finally, section 5 outlines our contributions and future work.

2. Background

2.1 Related Work

Risk analysis has always been a part of security design methods [4]. From a requirements perspective, reasoning about security risks is most naturally driven by threat analysis for real use cases. It includes scenario-based methods such as identifying misuse cases [41] [2], abuse cases [33], abuse frames [31] (based on problem frames [19]), and attack trees [40]. In contrast, goal-based methods often take an organizational perspective to reason about security risks, which include modeling of social relationships among actors/agents as soft-goals to be satisfied [32]; intruder anti-goal modeling [46]; and modeling risk as an event that prevents goal satisfaction [51]. The influence of Goal Question Metric (GQM) [3] is also seen on approaches for identifying the existence of security constraints throughout the organization [42] [21]. Viewpoint-based methods also advocate the identification of stakeholders with security viewpoints to minimize security risks [23]. Viewpoints are useful for identifying conflicts [15], which may lead to risks. Therefore, it is apparent that the selection of any single requirements method limits the factors taken into account for understanding the potential risks from the early stages of the system lifecycle. In addition, existing approaches rely heavily on the expertise of the analyst to trace and model interactions among system features [33] and then to reason about possible risks.

Frameworks for enterprise-level risk assessment, such as OCTAVE^{SM} [36], 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. Quantitative risk assessment approaches [17] [7] are usually manual, complicated, and rely on the subjective knowledge from experts and past experiences as they lack a baseline for systematically identifying potential risks in a given organizational environment.

SQUARE [34] includes risk assessment as a part of the requirements engineering process; however, it is loosely integrated with other parts of the methodology. Moffett et al [35], strongly express the need for integrating risk analysis into the requirements engineering process. We further suggest that in addition to application requirements, C&A requirements should be a key source of identifying dependability needs and conducting risk assessment during the requirements engineering process.

2.2 Modeling C&A Requirements

Before any analysis can be performed on C&A requirements in regulatory documents, it is necessary to identify the attributes that classify and categorize them from dimensions relevant to the problem solving activity. Robinson et al. [39] use requirements structuring and grouping for identifying requirements conflicts. Wasson [49] demonstrates that capturing various explications of concepts related to domain semantics helps to better manage the risk of mis-communication in requirements. Explication of obligations and rights from regulatory policies to clarify ambiguities is suggested by Travis et al. [6].

In our approach, rather than relying on any single modeling philosophy, 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. 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 [29]. Specifically, guided by the Ontology-based

ACTive Requirements Engineering (Onto-ActRE) framework [26], we harness the expressiveness of ontologies to classify and categorize C&A requirements from the dimensions: 1) a *requirements domain 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 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] [24] [28]; here we briefly elaborate on the process of analyzing a DITSCAP requirement to identify relevant risk components.

2.2.1 C&A Requirements & Risk Components

To support an overall risk-based strategy, C&A requirements should explicitly identify 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 [8]. The resulting model, as shown in Figure 1, explains the relationships between security requirements and risk components.

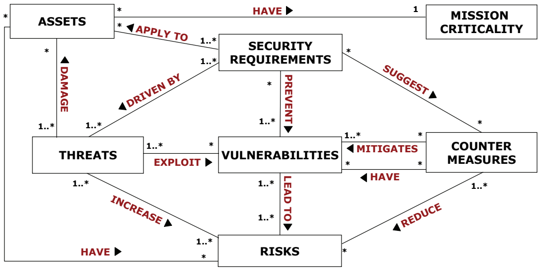


Figure 1: Requirements and Risk Model

Based on the model in Figure 1, 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. Figure 2 shows the explication of multi-dimensional domain concepts for the DITSCAP "Boundary Defense" requirement [12].

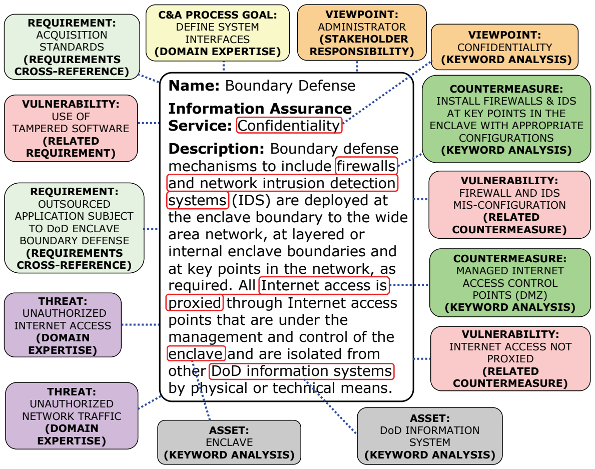

REQUIREMENT: ACQUISITION STANDARDS (REQUIREMENTS CROSS-REFERENCE)
C&A PROCESS GOAL: DEFINE SYSTEM INTERFACES (DOMAIN EXPERTISE)
VIEWPOINT: ADMINISTRATOR (STAKEHOLDER RESPONSIBILITY)
VIEWPOINT: CONFIDENTIALITY (KEYWORD ANALYSIS)
VULNERABILITY: USE OF TAMPERED SOFTWARE (RELATED REQUIREMENT)
COUNTERMEASURE: INSTALL FIREWALLS & IDS AT KEY POINTS IN THE ENCLAVE WITH APPROPRIATE CONFIGURATIONS (KEYWORD ANALYSIS)
REQUIREMENT: OUTSOURCED APPLICATION SUBJECT TO DoD ENCLAVE BOUNDARY DEFENSE (REQUIREMENTS CROSS-REFERENCE)
VULNERABILITY: FIREWALL AND IDS MIS-CONFIGURATION (RELATED COUNTERMEASURE)
COUNTERMEASURE: MANAGED INTERNET ACCESS CONTROL POINTS (DMZ) (KEYWORD ANALYSIS)
THREAT: UNAUTHORIZED INTERNET ACCESS (DOMAIN EXPERTISE)
VULNERABILITY: INTERNET ACCESS NOT PROXIED (RELATED COUNTERMEASURE)
THREAT: UNAUTHORIZED NETWORK TRAFFIC (DOMAIN EXPERTISE)
ASSET: ENCLAVE (KEYWORD ANALYSIS)
ASSET: DoD INFORMATION SYSTEM (KEYWORD ANALYSIS)
Name: Boundary Defense
Information Assurance Service: Confidentiality
Description: Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries and at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means.

Figure 2: Analyzing a DITSCAP Requirement

2.2.2 Evidences for Requirements Compliance

C&A activities require collecting supporting evidences from the target system to assess the level of compliance with C&A requirements. Therefore, 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 ordered levels of compliance prepared from the conjunction of criteria necessary to objectively reason about the level of compliance of the target system based on responses gathered from various resources [29].

3. Analyzing Correlations among C&A Requirements for Risk Assessment

During consultation with C&A practitioners (security consultants and experts), we perceive that their biggest problem is to be able to systematically reason about the collective adequacy of diverse security constraints towards emergent secure software behavior during operation, or lack thereof leading to potential security risks.

To this end, for a given scenario of the target system, our approach is to discover an exhaustive set of applicable security C&A requirements and construct a model of potential correlations among them. Based on metrics and measures available from the model, we convey: 1) The criticality of a particular class of security constraints on overall secure system behavior; and 2) The extent of potential risks due to correlations among a set of security constraints, imposed by applicable C&A requirements in a given scenario. We now detail the steps in our approach.

3.1 Step 1: Goal-driven Scenario Composition

To consider application requirements and real use cases, binding C&A to a certain environment (similar to USDA meat certification) has been suggested by Voas [48] for software systems. Correspondingly, we use operational scenarios of the target system as triggers for the discovery of applicable C&A requirements, ensuing risk assessment and negotiations during C&A activities in our approach. Operational scenarios of the target system can be easily obtained from domain experts and other artifacts (e.g. use cases). The CORAS framework [1] also advocates the use of mis-use cases [41] to provide a context for the risk assessment. Scenarios form the basis for providing a concrete understanding of abstract intentions of C&A requirements in the context of the target system.

Any requirements search or investigation process should have a goal or a set of goals [30]. Therefore, in this step, scenario composition is guided by the C&A process goals. A goal-driven approach helps to circumvent the problem of establishing the coverage of the identified scenarios over the large C&A requirements space. The output of this step is then a collection of scenarios driven by goals for understanding risks that a target system is subject to in its operational environment.

To demonstrate the feasibility of each step in our approach, as an example, consider the DITSCAP being applied to a hypothetical software information system that hosts a data repository for certain DoD missions. Driven by the C&A process goal for "Assessing System Interfaces" [11] the following operational scenario of the target system is composed by the analyst from remote access use case of the system:

> "*The target system enclave boundary enables remote access for all users with appropriate authentication and identification mechanisms.*"

In this scenario, an "*enclave*" refers to "collection of computing environments connected by one or more internal networks…" [11], whose examples include local area networks and the applications they host, backbone networks, and data processing centers. The "*enclave boundary*" refers to "the point at which an enclave's internal network service layer connects to an external network's service layer" [11].

3.2 Step 2: Formation of an Analysis Pool

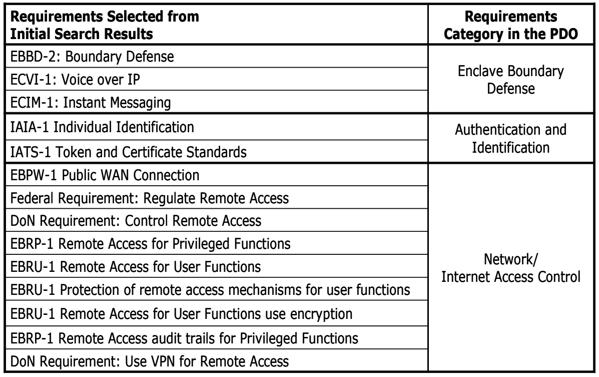
In this step, each operational scenario identified in the previous step drives the formation of an *Analysis Pool* of C&A requirements. We define analysis pool as an exhaustive compilation of C&A requirements that collectively constrain target system behavior in diverse ways in a socio-technical environment for a given operational scenario. Naturally, the membership of C&A requirements in an analysis pool is determined by the scenario and the goals of analysis.

To form an analysis pool it is important to facilitate the discovery of C&A requirements originating from distant sets or in different regulatory documents, but relevant to the current scenario. It concerns the 'requirements distance' problem [20], which is recognized as a non-trivial problem in software requirements engineering that cannot be handled well through a manual inspection of several natural language C&A requirements documents.

To address this problem, we apply a combination of search strategies on the requirements domain model of the PDO. It includes keyword-based search on C&A requirements modeled in the PDO (using SPARQL [38]), followed by focused hierarchical browsing (similar to file system browsing) of sibling and ancestor requirements, and finally exploring the multi-dimensional interdependencies that exist among requirements through other domain concepts in the PDO. Keyword-based search can be further augmented by query expansion [30] using related keywords in C&A guidance documents. The search strategies are applied incrementally to systematically expand (or contract) the search space of C&A requirements.

For the example scenario, keywords of "*enclave boundary*" "*remote access*" and "*authentication and identification*" are identified from the scenario description to apply the keyword-based search strategy. These keywords and their adjacent concepts in DITSCAP guidance documents are then used to search for C&A requirements in the PDO. The analyst examines the search results and interactively chooses only relevant C&A requirements for inclusion in the analysis pool. For example, the set of requirements chosen by the analyst are shown in Table 1.

Table 1: The Set of Requirements added to the Analysis Pool by Keyword-based Search Strategy



Requirements Selected from Initial Search Results	Requirements Category in the PDO
EBBD-2: Boundary Defense	Enclave Boundary Defense
ECVI-1: Voice over IP	
ECIM-1: Instant Messaging	
IAIA-1 Individual Identification	Authentication and Identification
IATS-1 Token and Certificate Standards	
EBPW-1 Public WAN Connection	Network/ Internet Access Control
Federal Requirement: Regulate Remote Access	
DoN Requirement: Control Remote Access	
EBRP-1 Remote Access for Privileged Functions	
EBRU-1 Remote Access for User Functions	
EBRU-1 Protection of remote access mechanisms for user functions	
EBRU-1 Remote Access for User Functions use encryption	
EBRP-1 Remote Access audit trails for Privileged Functions	
DoN Requirement: Use VPN for Remote Access	

Following the second search strategy, the analyst explores the siblings as well as ancestors of the requirements in Table 1, using a focused hierarchical browsing of the requirements domain model. The analyst discovers that requirements in the "Network/Internet Access Control" that are subsumed by requirements in the "Logical Access Control" category, are also applicable in the current scenario and are added to the analysis pool as shown in Table 2.

Table 2: The Set of Requirements added to the Analysis pool after expansion of the Search Space

Requirements Discovered through PDO Exploration	Requirements Category in the PDO	Method of Discovery in the PDO
ECLP-1 Privileged accounts assigned to privileged users	Logical Access Control	"Logical Access Control" category **subsumes** "Network/Internet Access Control" Category in the Requirements Domain Model of the PDO
ECLP-1 Least Privileges and Separation of duty		
ECLP-1 Privileged accounts limited to privileged functions		
DoN Requirement: Use Public Key Infrastructure		
Access Control for privileged users and IA officer	Personnel Screening	"Network/Internet Access Control" and "Personnel Screening" categories of the Requirements Domain Model are related through the **Viewpoint of "System Administrator"** in the Viewpoint hierarchy
IA Manager, IA Officer, and privileged users undergo security clearance		
ECTP-1 Audit Trail Protection	Audit Trails	"Network/Internet Access Control" and "Audit Trails" categories of the Requirements Domain Model are related through the **"requires"** relationship
ECAT-1 Audit Trail Monitoring, Analysis and Reporting		
EBVC-1 All VPN Traffic visible to IDS	Monitoring	"Enclave Boundary Defense" and "Monitoring" categories of the Requirements Domain Model share the **Countermeasure of "Install Firewalls and IDS at key points in the Enclave with appropriate configurations"** in the Countermeasure taxonomy
IAM, IAO and privileged users maintain knowledge of system	Security Awareness and Training	"Personnel Screening" and "Security Awareness and Training" categories of the Requirements Domain Model are related through the **Viewpoints of "System Administrator", "IAO" and "IAM"** in the Viewpoint hierarchy
DoN Requirement: Privileged users require Training		
DCSR-2 Specified Robustness	Product Specification and Evaluation	"Enclave Boundary Defense" and "Product Specification and Evaluation" categories of the Requirements Domain Model are related through the **"requires"** relationship
ECCT-1 Encryption for Confidentiality	Production, I/O Controls	"Enclave Boundary Defense" and "Production, I/O Controls" categories of the Requirements Domain Model are related through the **"requires"** relationship

Finally, as the third search strategy, the certification analyst examines the relationships of each requirement available in the analysis pool with other requirements in the requirements domain model, stakeholders in the viewpoint hierarchy, C&A process goals in the goal hierarchy, and risk components in the risk assessment taxonomy of the PDO. The analyst discovers that requirements in the "Network/Internet Access Control" category are related to requirements in the "Personnel Screening" category of the requirements domain model through the Viewpoint of "System Administrator" in the viewpoint hierarchy of the PDO, and are applicable in the current scenario. After a similar discovery process for other requirements, the C&A requirements shown in Table 2, are added to the analysis pool.

Here we emphasize that the analysis pool is in essence formed after a systematic exploration of C&A requirements space (based on a common understanding provided by the PDO) that spans stakeholder concerns from various levels in the organization for secure system operation in a given scenario.

3.3 Step 3: Abstractions in the Analysis Pools

For a given scenario, it is easy for the analyst to get lost in the details of a large number of applicable C&A requirements while missing the bigger picture, i.e. missing the forest for the trees. As systems get more complex, abstraction is a way to find correlations among requirements by ignoring some details. Specifically, the abstractions should help to highlight the correlations among different classes of constraints, imposed by C&A requirements, which collectively contribute to emergent secure software behavior.

To this end, we identify that each C&A requirements category in the requirements domain model embodies the general notion of constraints imposed on the software behavior by the C&A requirements that belong to each category. Therefore, in this step, each requirement in the analysis pool is abstracted to the most-specific parent requirement category in the requirements domain model of the PDO. Also, the relationships of each C&A requirement with risk components, as discussed in section 2.2.1, are now associated with the parent category of the C&A requirement due to the abstraction process.

For the example scenario, "Network/Internet Access Control" is the parent category for nine C&A requirements (Table 1) in the analysis pool. By abstraction, this requirement category then aggregates all the risk components identified for the nine requirements as shown Figure 3. Similarly, other sets of C&A requirements are also abstracted.

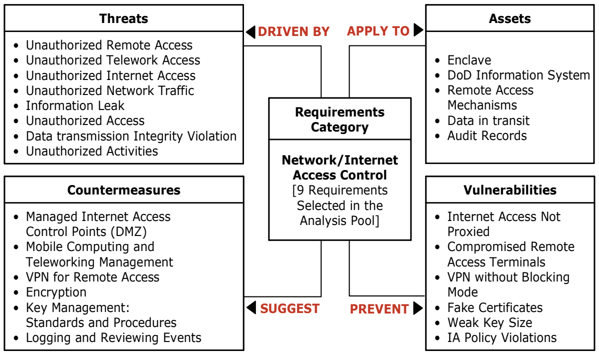

Threats
• Unauthorized Remote Access
• Unauthorized Telework Access
• Unauthorized Internet Access
• Unauthorized Network Traffic
• Information Leak
• Unauthorized Access
• Data transmission Integrity Violation
• Unauthorized Activities
DRIVEN BY
APPLY TO
Assets
• Enclave
• DoD Information System
• Remote Access Mechanisms
• Data in transit
• Audit Records
Requirements Category
Network/Internet Access Control
[9 Requirements Selected in the Analysis Pool]
Countermeasures
• Managed Internet Access Control Points (DMZ)
• Mobile Computing and Teleworking Management
• VPN for Remote Access
• Encryption
• Key Management: Standards and Procedures
• Logging and Reviewing Events
SUGGEST
PREVENT
Vulnerabilities
• Internet Access Not Proxied
• Compromised Remote Access Terminals
• VPN without Blocking Mode
• Fake Certificates
• Weak Key Size
• IA Policy Violations

Figure 3: Abstracting the Requirements

Despite these abstractions, traceable connections to the original C&A requirements in the analysis pool are always maintained. In addition, the corresponding evidences gathered using compliance questionnaires (Section 2.2.2) can be easily presented to the certification analyst as and when required.

3.4 Step 4: Creating a Model of Correlations

In this step, we construct an algebraic model of possible correlations among the C&A requirements in the analysis pool. To facilitate risk assessment, the model captures the correlations among C&A

requirements categories (representative of different classes of security constraints) from the dimensions of threats, assets, countermeasures, and vulnerabilities. Specifically, our approach is grounded in the algebraic framework of Formal Concept Analysis (FCA) [18].

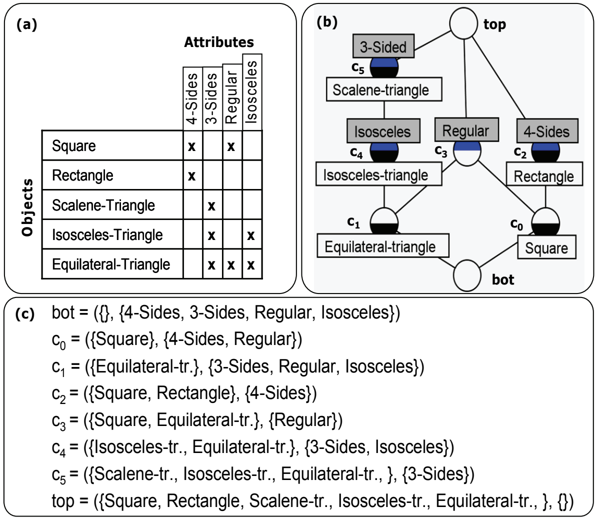
FCA formalizes the philosophical understanding of a "concept" as a unit of thought constituted by its extension and its intension. A *formal concept* binds these two components together in a *formal context* to allow fixing enough references for rationally interpreting them in human communication and argumentation [18]. It has been shown that FCA and logic systems based on semantic networks can be connected through their conceptual structures [50]. However, our goal here is not to compare *formal concepts* in FCA to domain concepts in the PDO. Rather, based on relationships among domain concepts modeled in the PDO, each *formal concept* in the FCA algebraic model includes C&A requirements and their compliance evidences as its extension (connections to reality); and its intention (human thinking/semantics) as meaningful combinations of risk components.

3.4.1 Formal Concept Analysis Overview

FCA defines a *formal context* (G, M, I) as a set G of *formal objects*, a set M of *formal attributes*, and a binary relation $I \subseteq G \times M$ indicating which *formal object* has which *formal attribute*. Within a *formal context*, a *formal concept* c is defined as a pair of sets (A, B) forming a Galois connection such that:

$$A = \{g \in G \mid \forall m \in B: (g, m) \in I\}.$$
$$B = \{m \in M \mid \forall g \in A: (g, m) \in I\}.$$

where the set A of *formal objects* is the extent and set B of *formal attributes* is the intent of *formal concept* c.



Objects	4-Sides	3-Sides	Regular	Isosceles
Square	x		x	
Rectangle	x			
Scalene-Triangle		x		
Isosceles-Triangle		x		x
Equilateral-Triangle		x	x	x

bot = ({}, {4-Sides, 3-Sides, Regular, Isosceles})
c_0 = ({Square}, {4-Sides, Regular})
c_1 = ({Equilateral-tr.}, {3-Sides, Regular, Isosceles})
c_2 = ({Square, Rectangle}, {4-Sides})
c_3 = ({Square, Equilateral-tr.}, {Regular})
c_4 = ({Isosceles-tr., Equilateral-tr.}, {3-Sides, Isosceles})
c_5 = ({Scalene-tr., Isosceles-tr., Equilateral-tr., }, {3-Sides})
top = ({Square, Rectangle, Scalene-tr., Isosceles-tr., Equilateral-tr., }, {})

Figure 4: (a) Example of a Formal Context; (b) Concept Lattice; and (c) Formal Concepts

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. Their relation is shown as (A, B) ≤ (C, D). A partially ordered set of all *formal concepts* is always a complete lattice structure and is called a *concept lattice*.

An example *formal context* and its relation; its concept lattice and *formal concepts* are shown in Figure 4 (a), (b), and (c) respectively (adapted from [43]). Within the concept lattice it is possible to annotate nodes representative of formal concepts in a concise way, which can be seen in the correspondence between the concepts in Figure 4 (b) and Figure 4 (c).

3.4.2 Constructing a Formal Context

Most FCA applications are selectively and opportunistically driven [22], which creates problems for understanding when and how to apply FCA. To address this issue, in our approach we innovatively use the security requirements and risk model, as shown in Figure 1, to guide the formation of *formal contexts*.

The model in Figure 1 helps to formulate four interesting cases for risk assessment: 1) A *Threat Assessment Case* to know which requirements are "*driven by*" a shared set of Threats to Assets that are applicable to; 2) A *Vulnerability Assessment Case* to know which requirements collectively try to "*prevent*" exploitable Vulnerabilities in Assets that are applicable to; 3) A *Countermeasure Assessment Case* to know which requirements "*suggest*" to collectively enforce a set of Countermeasures for the Assets that are applicable to; and 4) A *Risk Assessment Case* to know which requirements are "*driven by*" a shared set of Threats that can "*damage*" Assets by "*exploiting*" Vulnerabilities; and the Countermeasures "*suggested*" by requirements to mitigate the Vulnerabilities.

To systematically answer these questions using FCA, the requirements categories in an analysis pool are interpreted as *formal objects*, related risk components as *formal attributes*, and their relationships (dyadic predicates, e.g. *driven_by* {C&A requirement, Threat}) are recorded as crosses in the *formal context relation*. For the example scenario, the "Network/Internet Access Control" requirement category forms a *formal object*, its related risk components (as shown in Figure 3) form the *formal attributes* based on the selected assessment case, and their relationships are depicted as a cross in the *formal context* relation. Similarly, other requirement categories and related risk components in the analysis pool are added to the *formal context*.

For the Risk Assessment Case, in the example scenario, a *formal context* is prepared in Figure 5. Patterns of significant interactions among different classes of constraints on system behavior, now readily become apparent from the dimensions of risk components necessary for risk assessment.

Legend
R: Requirement Categories
T: Threats
A: Assets
C: Countermeasures
V: Vulnerabilities

	T1: Public IM Traffic	T2: Public VoIP Traffic	T3: Unauthorized Network Traffic	T4: Unauthorized Internet Access	T5: Unauthorized Access	T6: Employee Related Unauthorized Access	T7: Unauthorized Remote Access	T8: Unauthorized Telework Access	T9: Information Leak	T10: Data Transmission Integrity Violation	T11: Untrained Personnel	T12: Data at Rest Integrity Violation	T13: Unauthorized Activities	A1: Enclave	A2: DoD Information System	A3: Data	A4: Data in Transit	A5: Audit Records	A6: Remote Access Mechanisms	A7: Software	A8: Firmware	A9: Hardware	A10: Control Data
R1: Production and I/O Controls										X				X	X	X	X						
R2: Product Specification and Evaluation										X				X	X	X	X						
R3: Enclave Boundary Defense	X	X	X	X									X	X	X								
R4: Network/Internet Access Control			X	X	X	X	X	X	X	X			X	X	X	X	X	X	X				
R5: Monitoring					X		X						X	X	X								
R6: Audit Trail												X	X	X	X			X					
R7: Security Awareness and Training											X			X	X								
R8: Authentication and Identification					X								X	X	X								
R9: Logical Access Control					X	X							X	X	X								
R10: Personnel Screening						X							X	X	X	X				X	X	X	X

	C1: Monitor Installed Software	C2: Install Firewall and IDS	C3: Managed Internet Access Points	C4: User Password Management	C5: Key Mgmt.: Protection of Crypt. Keys	C6: Key Mgmt.: Standards and Procedures	C7: Privilege Management	C8: Personnel Screening	C9: Mobile Computing Mgmt.	C10: VPN for Remote Access	C11: Encryption	C12: Logging and Reviewing Audit Trails	C13: Education and Training	C14: Use of Certified COTS IA products	V1: Firewall and IDS Mis-configuration	V2: Tampered Software	V3: Internet Access Not Proxied	V4: Fake Certificates	V5: Weak Key Size	V6: Password-based Authentication Vuln.	V7: Excess privileges	V8: Conflict of Interest	V9: insufficient Background Checks	V10: Compromised Remote Access Terminals	V11: VPN without Blocking Mode	V12: IA Policy Violations	V13: Lack of Training
R1: Production and I/O Controls											X							X	X								
R2: Product Specification and Evaluation						X					X			X		X		X	X								
R3: Enclave Boundary Defense	X	X	X												X	X	X										
R4: Network/Internet Access Control			X		X	X	X	X	X	X	X	X					X	X	X		X	X	X	X	X	X	
R5: Monitoring		X								X					X										X		
R6: Audit Trail												X														X	
R7: Security Awareness and Training													X														X
R8: Authentication and Identification				X	X	X												X	X	X							
R9: Logical Access Control					X	X	X	X										X	X		X	X	X				
R10: Personnel Screening							X	X													X		X				

Figure 5: Formal Context for the Risk Assessment Case

3.4.2.1 Augmenting the Formal Context

The *formal context* can be augmented based on the domain semantics available from the PDO. Specifically, the hierarchical "is-a" relationships among C&A requirements categories as well as among risk components in the PDO, can be used to augment the *formal context* for making valuable inferences about possible correlations. Nevertheless, domain semantics should be preserved across the knowledge representation of the PDO and the *formal context* [5] [22] even after augmentation. Ontological concepts in the PDO are hierarchically related based on their level of abstraction; whereas, the concept hierarchy (partial order) in the FCA concept space is purely based on the containment relationship between *formal concept extents* or *intents*. Therefore, for the *formal objects* or *formal attributes,* that are ontological concepts with subsumption relationship among them in the PDO, we augment the *formal context* based on the rules that preserve the domain semantics reflected in the PDO with the *formal concepts* and their partial order.

The augmentation rule for capturing inheritance relationship between the *formal objects* (requirements categories in the PDO) is: Given that $g1, g2 \in G$, $m \in M$ and *sub-class (g1, g2)* means *g1* is subsumed by *g2,*

$$\boxed{\textit{sub-class}\ (g1, g2) \wedge ((g2, m) \in I)) \rightarrow ((g1, m) \in I)}$$

Based on this rule, in Figure 5, since the *formal object* of "Network/Internet Access Control" is subsumed by "Logical Access Control" in the requirements domain model of the PDO, the former participates in all the relationships with risk components (*formal attributes*) that the latter participates in. As a result, the vulnerability of "Excess Privileges" related to "Logical Access Control" is now extended into the context of "Network/Internet Access Control" category. This helps to infer the cascading effect of failure in the "Personnel Screening" category (related to "Excess Privileges" vulnerability) in the context of "Network/Internet Access Control" category.

Similarly, the augmentation rule for capturing inheritance relationship between the *formal attributes* (risk components in the PDO) is: Given $g \in G$ and $m1, m2 \in M$

$$\boxed{\textit{sub-class}\ (m1, m2) \wedge ((g, m1) \in I)) \rightarrow ((g, m2) \in I)}$$

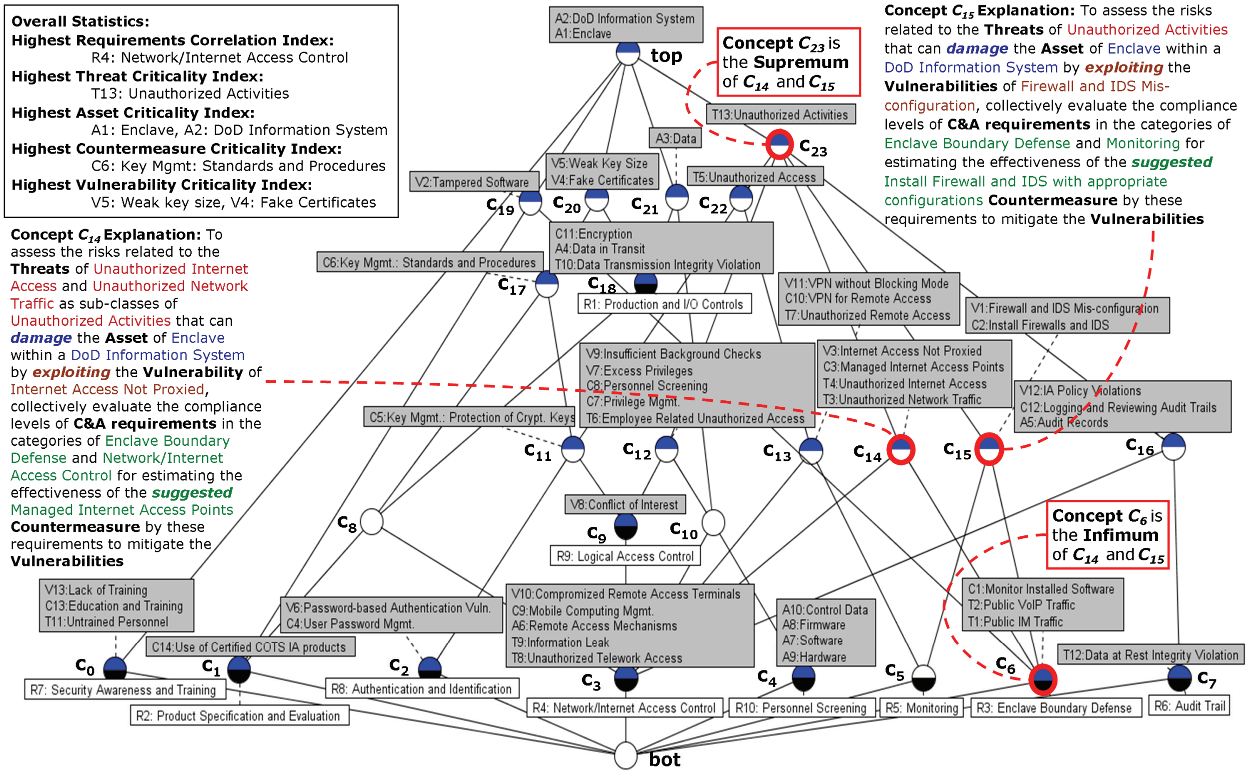
Based on this rule, in Figure 5, since the *formal attribute* of "Data in Transit" is subsumed by "Data" in the Asset taxonomy of the PDO, all requirements categories (*formal objects*) that participate in a relationship with the former also participate with the latter. As a result, the requirement categories of "Network/Internet Access Control", "Product Specification and Evaluation", and "Production and I/O Controls" related to "Data in transit" are now extended into the context of "Data". This helps to infer the cascading effect of failure in the "Personnel Screening" category (which is also related to the asset of "Data") on the multi-dimensional constraints imposed by various requirements categories that are now understood to be collectively contributing to projecting the asset of "Data" in the given scenario.

Thus, augmenting the *formal context* using domain semantics helps to systematically perceive the true extent of the risk assessment problem space.

3.4.2.2 The Concept Lattice of a Formal Context

The partially ordered set of all *formal concepts* in Figure 5 is shown in Figure 6 as a complete lattice. The *concept lattice* provides a compact and visual representation to analyze all potential correlations among C&A requirements categories in the given scenario, while facilitating their interpretation for risk assessment. The explanations of *formal concepts* "C14" and "C15" as shown in Figure 6 are generated by systematically interpreting their intents and extents based on the requirements and risk model in Figure 1.

The understanding of *formal concepts* developed based on concrete references in the given situated problem concept space helps certification analysts to rationally interpret the “*necessity and sufficiency*” of a set of correlated security constraints imposed by C&A requirements in addressing the risks perceived.



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_{14} Explanation: To assess the risks related to the **Threats** of Unauthorized Internet Access and Unauthorized Network Traffic as sub-classes of Unauthorized Activities that can ***damage*** the **Asset** of Enclave within a DoD Information System by ***exploiting*** the **Vulnerability** of Internet Access Not Proxied, collectively evaluate the compliance levels of **C&A requirements** in the categories of Enclave Boundary Defense and Network/Internet Access Control for estimating the effectiveness of the ***suggested*** Managed Internet Access Points **Countermeasure** by these requirements to mitigate the **Vulnerabilities**

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}

A2:DoD Information System
A1:Enclave
top
T13:Unauthorized Activities
A3:Data
C23
V5:Weak Key Size
V4:Fake Certificates
T5:Unauthorized Access
V2:Tampered Software
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
C8
V8:Conflict of Interest
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
R8: Authentication and Identification
R2: Product Specification and Evaluation
R4: Network/Internet Access Control
R10: Personnel Screening
R5: Monitoring
R3: Enclave Boundary Defense
R6: Audit Trail
bot

Figure 6: Concept Lattice for the formal context shown in Figure 5

3.5 Step 5: Metrics and Measures

The concept lattice of any *formal context* is complete, and each arbitrary collection of *formal concepts* has a greatest common subconcept (infimum) and a least common superconcept (supremum) [18].

Based on our application of FCA, these algebraic operations on *formal concepts* help to develop the following metrics and measures in a given scenario:

– ***Risk upper bound due to correlation among any arbitrary number of chosen requirement categories***: It is identified by computing the supremum of the most specific *formal concepts* related to the chosen requirements categories. The combination of risk components in the intent of the supremum expresses the upper bound of risks due to non-compliance in the chosen requirements categories. The collection of requirements categories in the extent of the supremum expresses the maximum possible propagative effect due to non-compliance in the chosen requirements categories, which lead to the risk upper bound.

– ***Risk lower bound due to correlation among any arbitrary number of chosen requirement categories***: It is identified by computing the infimum of the most specific *formal concepts* related to the chosen requirements categories. The combination of risk components in the intent of the infimum expresses the lower bound of risks due to non-compliance in the chosen requirements categories. The collection of requirements categories in the extent of the infimum expresses the minimum possible propagative effect due to non-compliance in the chosen requirements categories, which lead to the risk lower-bound.

– ***Requirement Category Correlation Index***: It is generated by dividing the number of occurrences of a requirement category in the extent of all *formal concepts* in the lattice, with the total number of *formal concepts*. In the range of [0, 1], higher the index of a requirement category, higher is the potential for its correlation with other requirements categories.

– ***Risk Component Criticality Index***: It is generated by dividing the number of occurrences of a risk component in the intent of all *formal concepts* in the lattice, with the total number of *formal concepts*. In the range of [0, 1], higher the index for a risk component, higher is its dependency on the collective compliance in many requirements categories. This index is maintained for each type of risk component.

With some practice, metrics for risk upper and lower bounds can also be visually computed by selecting two or more nodes in the concept lattice. For example by selecting the nodes "C14" and "C15," correlations among the requirements categories in the union of their extents can be examined. Therefore, the risk upper bound for "Enclave Boundary Defense," "Monitoring," and "Network/Internet Access Control" requirement categories can be computed by identifying the supremum of nodes "C14" and "C15", which is the lowest common node reached via ascending paths from both nodes, that is, node "C23." From its intent, we understand that the risk upper bound as the Threat of "Unauthorized Activities" to the Assets of "Enclave" within the "DoD Information System." The collection of "Logical Access Control," "Authentication and Identification," "Personnel Screening," "Audit Trails," "Enclave Boundary Defense," "Monitoring," and "Network/Internet Access Control" in its extent expresses the maximum possible propagative effect due to non-compliance in the chosen requirements categories, which lead to the risk upper bound. The certification analyst can now objectively reason about possible risks by examining the evidences gathered using compliance questionnaires (section 2.2.2) for C&A requirements in these categories. In addition, generic risk components in the PDO can be mapped to real world entities of the target system to reflect the subjective criticality of risk components. For example, the asset of "Data in Transit" can be mapped to "Secret Policies" and the threat of "Data transmission Integrity Violation" can be mapped to "Hackers of Foreign Countries" in a particular scenario of the target system.

Also, other metrics discussed in this section are used to prioritize C&A requirements and risk components in a given scenario as shown in Figure 6.

3.5.1 The Implication Rules of a Formal Context

In a *formal context*, an implication between subsets of *formal attributes* is denoted by A → B, where the attribute set A is the *premise* and attribute set B is the *conclusion*. An implication holds in a *formal context* if each *formal object* that is related to the attribute set in the premise is also related to the attribute set in the conclusion. Although the number of possible implications can be very large, a stem base [14] with the fewest number of implications exists from which all other implications can be derived. The stem base is sound, complete and non-redundant. Interestingly, the set of *formal attributes* in any implication of the stem base corresponds to the intent of a *formal concept*.

In our approach, implications in a *formal context* correspond to possible implications between risk components in the given scenario. Therefore, from a risk assessment perspective, if the stem base of implications among risk components is demonstrated to be mitigated based on evidences gathered for C&A requirements (in the extent of each *formal concept*), then all possible implications among risk components can be assured to be covered (mathematically 100% risk coverage) in the given situated problem space. On the other hand, all possible implications among risk components due to non-compliance with C&A requirements also become apparent.

4. C&A Documentation Artifacts

Typical for most C&A approaches, DITSCAP requires extensive paperwork to produce a single System Security Authorization Agreement (SSAA) document. Although many task reports related to risk assessment are prepared by executing DITSCAP activities, the SSAA outline only includes a "Section 2.3 Threat Description" in the main document, and the "Residual Risk Assessment Results" section as appendix. It is left entirely up to the discretion of the certification analyst to manage, analyze and document the results of risk assessment. As a result, despite risk assessment activities being spread throughout the DITSCAP, they are only superficially interleaved with security C&A requirements related activities. To this end, the risk assessment artifacts resulting from our step-wise methodology make several contributions:

- Risk assessment is tightly integrated with the process of understanding C&A requirements applicability and compliance in the context of the target system.
- Well-defined metrics and measures facilitate an overall risk-based strategy to prioritize C&A requirements compliance efforts from the early stages of the software lifecycle
- Visual illustrations are accessible to diverse stakeholders for understanding C&A documentation
- Well-defined artifacts act as a baseline to guide the creation of task reports required for various C&A risk assessment activities. For example, various analysis pools provide a baseline to justify the threat descriptions task reports and vice versa.
- Combined understanding of the technical and non-technical security constraints in the context of operational system scenarios of the real world. For example, the impact of technical vulnerabilities identified in the "Vulnerability Assessment Task Report" in the DITSCAP SSAA [10] can be understood in context of relevant analysis pools.

5. Contributions and Future Work

We presented a C&A requirements-driven approach to risk assessment for complex software systems. Our approach facilitates the discovery of an exhaustive set of C&A requirements applicable in a given operational scenario of the target system, and understanding of their correlations with application to risk assessment. The FCA algebraic model of correlations among C&A requirements categories facilitates the development of metrics that help to prioritize their value towards "risk-free" secure system behavior in a given scenario.

We identify that, as an assortment of analysis pools become available, recurring structures in their correlation model (*formal concepts* of FCA) can help to detect interactions across scenarios. Presently, we are investigating these analogical correlations to reveal unexpected interactions among scenarios. Our ongoing and future work also focuses on making available an integrated requirements-driven C&A workbench to support the methodology presented in this paper [25]. In addition to risk assessment, we expect to provide a more general approach to analyze correlations among requirements based on diverse modeling artifacts made available in a socio-technical environment.

6. References

[1] Aagedal, J.O., den Braber, F., et al., "Model-based risk assessment to improve enterprise security," In Proc. of the 6th Int'l Enterprise Distributed Object Computing Conf., 2002, pp: 51 – 62.

[2] Alexander, I. "Misuse Cases: Use Cases with Hostile Intent." IEEE Software, 20(1), Jan/Feb 2003, pp: 58-66.

[3] Basili V.R., Rombach H.D., "The TAME project: Towards improvement-oriented software environments," IEEE Transactions on Software Engineering, 14(6), 1988, pp: 758-773.

[4] Baskerville, R., "Information systems security design methods: implications for information systems development," ACM Computing Surveys, 25(4), 1993, pp: 375-414.

[5] Borgida, A. "On the Relative Expressiveness of Description Logics and Predicate Logics," AI, 82(1-2), 1996, pp: 353–367.

[6] 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.

[7] Butler, S.A. "Security Attribute Evaluation Method: A Cost Benefit Approach." 24th Int'l Conf. Soft. Eng., 2002, pp: 232-240.

[8] Common Criteria, v2.1. ISO/IEC 15408-1, 1999.

[9] Davis T., "Federal Computer Security Report Card Grades of 2004," Press Release. Government Reform Committee, 2005.

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

[11] DoD Instruction 5200.40: DITSCAP, 1997.

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

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

[14] Duquenne, V. "Contextual implications between attributes and some representational properties for finite lattices" Beitrage zur Begrisanalyse, B.I. Wissenschaftsverlag, 1987, pp: 213-239

[15] Easterbrook, S., "Domain modelling with hierarchies of alternative viewpoints", In Proc. Int'l Sym. on RE., 1993, pp: 65-72.

[16] Ernst & Young, "Report on the Widening Gap," 8th annual Global Information Security Survey, Netherland, 2005.

[17] Feather, M. S., Cornford, S.L., "Quantitative risk-based requirements reasoning," *RE Journal*, Vol. 8(4), 2003, pp: 248-265.

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

[19] Jackson, M., *Software Requirements and Specifications: A Lexicon of Practice, Principles and Prejudices*. Addison, 1995.

[20] Jilani, L.L., et al., "Defining and applying measures of distance between specifications," *IEEE TSE*, 27(8), 2001, pp.673-703.

[21] Johansson E, Johnson P. "Assessment of Enterprise Information Security - Estimating the Credibility of the Results," In Proc. Sym. on RE for Info. Security (SREIS 05) at RE 05, 2005.

[22] Kalfoglou, Y., Dasmahapatra, S. Chen-Burger, J., "FCA in Knowledge Technologies: Experiences and Opportunities," In Proc. 2nd Int'l Conf. on FCA, 2004, pp: 252-260.

[23] Kotonya, G., Sommerville, I., "Requirements engineering with viewpoints," Software Engineering Journal, 11(1), 1996, pp: 5-18.

[24] Lee, S.W., Gandhi, R.A. et al, "Security Requirements Driven Risk Assessment for Critical Infrastructure Information Systems", In Proc. Sym. on RE for Info. Security (SREIS 05) at RE 05, 2005.

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

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] Lee, S.W., Rine, D.C. "Missing Requirements and Relationship Discovery through Proxy Viewpoints Model," Studia Informatica Universalis: Int'l Journal on Informatics, 3(3), 2004 pp. 315-342.

[31] Lin, L., Nuseibeh, B., Ince, D., Jackson, M., "Using abuse frames to bound the scope of security problems," In Proc. of the 12th Int'l Conf. on Requirements Engg, 2004, pp: 354- 355.

[32] Liu, L., Yu, E., Mylopoulos, J., "Security and Privacy Requirements Analysis within a Social Setting," In Proc. of the 11th Int'l Conf. on Requirements Engg, 2003, pp: 151-161.

[33] McDermott, J. "Abuse-Case-Based Assurance Arguments," In Proc. 17th Comp. Security App. Conf., IEEE CS, 2001, pp: 366-374

[34] Mead, N.R., Hough, E., Stehney, T., "Security Quality Requirements Engineering (SQUARE) Methodology," Technical Report (CMU/SEI-2005-TR-009), SEI, CMU, Pittsburgh, PA 2005

[35] Moffett, J.D., Haley, C.B., Nuseibeh, B.A, "Core Security Requirements Artefacts," TR 2004/23, Open University, June 2004.

[36] OCTAVE^{SM} Criteria v2.0, CMU/SEI-2001-TR-016, 2001.

[37] Prieto-Diaz, R., "The Common Criteria Evaluation Process," CISC-TR-2002-003, James Madison Univ., 2002.

[38] Prud'hommeaux, E., Seaborne, A., "SPARQL Query Language for RDF," W3C Working Draft, 2006.

[39] Robinson W.N., Pawlowski, S., "Surfacing Root Requirements Interactions from Inquiry Cycle Requirements," In Proc. 6th Int'l Conf. on RE, 1998, pp. 82-89.

[40] Schneier, Bruce. "Attack Trees." Dr. Dobb's Journal of Software Tools, 24(12), December 1999, pp: 21-29.

[41] Sindre, G., Opdahl, A., "Eliciting Security Requirements by Misuse Cases," In Proc. of TOOLS Pacific, 2000, pp: 120-130.

[42] Swanson M, Bartol N, et al., "Security Metrics Guide for Information Technology Systems," NIST SP #800-55, 2003.

[43] Tonella, P., "Reverse Engineering of Object-Oriented Code," Mini-tutorial 27th Int'l Conf. on Soft. Engg., St. Louis, 2005.

[44] US GAO Report, "Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation," 04-376, 2004.

[45] US GAO Report, "Department of Homeland Security Needs to Fully Implement its Security Program," 05-700, 2005.

[46] van Lamsweerde, A., "Elaborating Security Requirements by Construction of Intentional Anti-Models," In Proc. 26th Int'l Conf. on Software Engg., 2004, pp: 148-157.

[47] Verdon, D., McGraw, G., "Risk Analysis in Software Design." IEEE Security & Privacy Magazine, 2(4), 2004, pp: 79-84

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

[49] Wasson, K. S., "A Case Study in Systematic Improvement of Language for Requirements," 14th Int'l RE Conf., 2006, pp: 6- 15.

[50] Wille, R., "Conceptual Graphs and Formal Concept Analysis," Int'l Conf. on Conceptual Structures, 1997, pp: 290-303.

[51] Yudistira, A., Giorgini, P., Mylopoulos, J., "Risk Modelling and Reasoning in Goal Models," DIT-06-008, Univ. of Trento, 2006.