In Proceedings of the Third Int'l Workshop on Software Engineering for Secure Systems (SESS 07)
in conjunction with the 29th International Conference on Software Engineering (ICSE 07),
Minneapolis/St. Paul, MN, USA. IEEE Press. May 19-20.

Towards a Requirements-driven Workbench for Supporting Software Certification and Accreditation

[Short presentation paper]

Seok-Won Lee, Robin A. Gandhi and Siddharth Wagle
Knowledge-intensive Software Engineering Research Group
Dept. of Software and Information Systems, University of North Carolina at Charlotte
Charlotte, NC 28223-0001, USA. {seoklee,rgandhi,sjwagle} @uncc.edu

Abstract

Security certification activities for software systems rely heavily on requirements mandated by regulatory documents and their compliance evidences to support accreditation decisions. Therefore, the design of a workbench to support these activities should be grounded in a thorough understanding of the characteristics of certification requirements and their relationships with certification activities. To this end, we utilize our findings from the case study of a certification process of The United States Department of Defense (DoD) to identify the design objectives of a requirements-driven workbench for supporting certification analysts. The primary contributions of this paper are: identifying key areas of automation and tool support for requirements-driven certification activities; an ontology-driven dynamic and flexible workbench architecture to address process variability; and a prototype implementation.

1. Introduction

A recent survey [7] – 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. For example, the United States Office of Management and Budget stresses that funding can be potentially denied for those IT investments that do not meet security certification requirements, prior to becoming operational [27] [24].

Software security certification is defined as the 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 dependability requirements [6]. Activities throughout the C&A process lifecycle rely heavily on decision points for interpretation, applicability, scope and evaluation of certification requirements [21] [13], while assessing the security risks due to non-compliance [16]. In addition, C&A related documentation often attempts to capture the artifacts produced throughout the C&A process as a single text document to guide secure software engineering activities, document decisions, specify requirements, certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security [6].

Regulatory C&A requirements are mandated to be complied with if found applicable to certain aspect of software behavior in its operational profile. However, C&A requirements are generally non-functional and scattered across many natural language regulatory documents that reflect the interests of multiple stakeholders from various levels in the organization. The nature of current software systems, as highly interconnected systems of systems operational within diverse socio-technical environments, further aggravate the issues related to the C&A process.

It is now becoming increasingly difficult to justify the necessity and sufficiency of the multi-faceted constraints imposed on software system behavior by regulatory certification requirements. Various reports [4] [27] [11] [28] indicate that the process of measuring software system compliance with certification requirements is often irregular and unreliable in actual practice. Consequently, 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 [27] [28].

To address the issues discussed here, our research efforts have been focused towards modeling certification requirements based on a requirements engineering framework that facilitates a common understanding of C&A requirements among stakeholders. Our approach has been applied to the Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP) [6] with promising preliminary results [19] [18] [20] [21].

In this paper we utilize the findings from the case study of DITSCAP to outline the design objectives of a requirements-driven workbench for supporting C&A activities. One of the primary contributions of this paper is in identifying the C&A activities that can be effectively carried out based on a structured and common understanding of C&A requirements.

As technology evolves, it allows more and more dynamic inter-connectivity among systems. A workbench to support the C&A process has to consider the needs for flexible delivery of C&A process artifacts on-demand in a highly interconnected environment. It is important to note that despite corresponding variations in the C&A process definition for such environments, the foundational organizational concerns for software assurance embedded in C&A requirements do not change significantly. For example, the recent transition of DITSCAP to DIACAP [30], geared towards net-centric infrastructure, implies change in process and the format of delivery and consumption of C&A artifacts; but, they still significantly overlap over the set of documents suggested for identifying C&A requirements. To consider these issues during the design of a requirements-driven C&A workbench, we leverage a unique combination of service and aspect-oriented design paradigms.

The paper is organized as follows. Section 2 discusses the state of current commercial tool support for C&A. Section 3 provides a brief introduction to DITSCAP and related aspects of our previous research efforts to this paper. In Section 4, we identify the design objectives of a generic requirements-driven C&A workbench and elaborate upon them. Section 5 discusses different parts of flexible and dynamic workbench architecture along with a snapshot of our current prototype implementation. We discuss our contributions and future work in Section 6.

2. Commercial Tool Support for C&A

Several commercial tool support and services exist; however, they use proprietary methods and procedures which are usually not available to the research community for evaluation. In our experience with trial versions and demos of popular commercial tools such as Telos Xacta IA manager [32], I-Assure autoRTM [12], and Secureinfo Compliance Authority tool [25], they offered wizard based questionnaires with automated documentation generation capabilities; but lacked specific focus on stakeholder understanding of the C&A process, and individual C&A requirements in the context of the target system and environment.

These tools provide a structured and easily accessible database of security requirements, extracted from C&A documents. However, little or no guidance is offered to understand various aspects of the constraints imposed by C&A requirements on the target system behavior and risks related to non-compliance. As a result, the C&A process often merely reduces to a checklist exercise for generating C&A documentation, but without a thorough understanding of the operational risks of the site and the system.

3. Background

For the DoD, security is a key dependability attribute for software systems. The DITSCAP [6] ensures that DoD dependability needs are uniformly considered throughout the lifecycle of all information systems that support information processing services within the DoD information infrastructure (DII).

However, DITSCAP has several limitations. Practicing DITSCAP requires significant familiarity with several guidance documents from different levels in the DoD organizational hierarchy to identify the applicable set of security requirements necessary for certification. Each document usually ranges between 25 and 200 pages with heavy cross-referencing to other documents. Within these documents, natural language C&A requirements have very little or no structural regularity in their specifications. In addition, numerous C&A requirements reflect stakeholder interests from different levels in the organization.

To address these issues, our research efforts are focused on effectively modeling C&A requirements. Specifically, the Ontology based ACTive Requirements Engineering (Onto-ActRE) framework [17], harnesses the expressiveness of ontologies [26] to utilize the synergy among multiple requirements engineering modeling philosophies for effectively representing and modeling C&A requirements [14].

The Onto-ActRE approach to ontology development is primarily problem driven; its creation is guided based on the problem solving notions of goals, scenarios, and viewpoints (requirements engineering techniques). Driven by these modeling philosophies, we extract ontological concepts from natural language C&A guidance documents as well as domain experts to help in classifying and categorizing C&A requirements from multiple dimensions [21].

The resulting Problem Domain Ontology (PDO) includes the following dimensions: 1) a hierarchical requirements domain model of various requirement types that categorize 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 gather user/system criteria for C&A requirements applicability; 4) domain specific taxonomies with ontological concepts in the dimensions of threats, countermeasures, vulnerabilities, and assets related to C&A requirements for understanding risks associated with non-compliance; and 5) interdependencies among concepts modeled in the PDO. Further details about these models are described in [20].

Semantics of C&A requirements are now reflected by their relationships with other concepts in the PDO along with capabilities for visual analytics [29].

Support for object-oriented ontological domain modeling is provided by the GENeric Object Model (GenOM) [15] toolkit. GenOM inherits the theoretical foundation of the frame representation and is compatible with the OKBC specification [2].

4. C&A Workbench Design Objectives

Based on our approach to model C&A requirements, we now outline the key design objectives of a requirements-driven workbench for supporting C&A activities. We identify the shortcomings of the current manual C&A approaches and then propose ways in which they can be supported by providing the context of and traceability to C&A requirements modeled in a PDO.

4.1 C&A Process Guidance

C&A is a long and exhaustive process based on a set of activities defined in C&A guidance documents. However, in order to maintain general applicability the process definition is often loosely related to the C&A requirements specified in other regulatory documents. For example, in the DITSCAP application manual [5] each activity definition entails the processing of certain C&A requirements in the context of the target system; but, due to lack of explicit traceability between DITSCAP activities and relevant certification requirements, stakeholders often find it hard to gauge certification progress and determine the coverage of activities over the space of requirements.

To address these issues, the first design objective of the requirements-driven C&A workbench is to provide active process guidance to stakeholders. In this direction, we have established explicit traceability between concepts in the C&A process goal hierarchy and each C&A requirement categorized in the requirements domain model of the PDO. This traceability provides the ability to increase C&A process understanding based on metrics for 1) C&A progress; 2) C&A task complexity; 3) Domain coverage of a C&A task; and 4) Task interdependencies. These metrics also complement any process workflow visualization techniques that may be adopted, to provide real-time updates based on changes in the compliance status of C&A requirements.

4.2 Understanding C&A Requirements

Security by its nature requires a broad spectrum of knowledge and system information. However, during C&A we often have to rely on the domain knowledge and experience of subject matter experts to make decisions regarding the completeness of identified C&A requirements leading to subjective decisions. Also, generating a Requirements Traceability Matrix (RTM) of applicable C&A requirements is a long and tedious process prone to error as it requires sifting through a multitude of C&A related documents and comprehending their interdependencies. In addition, non-functional certification requirements often constrain diverse aspects of information system behavior in complex ways that are not readily apparent from their natural language descriptions.

These issues motivate the design objectives for providing techniques to understand C&A requirements and the criteria to assess their applicability. To this end, the inherent structure of the PDO provides a systematic way to understand C&A requirements. For example, the requirements domain model of DITSCAP hierarchically organizes requirements enforced through the top-level generic Federal laws, mid-level domain spanning DoD policies, and leaf-node DoD/DoN sub-domain site/agency specific requirements and implementations. Such organization of requirements allows for their exploration to be conservative in nature i.e. to be more inclusive rather than exclusive. In addition, the semantics and applicability of each C&A requirement can be evaluated by its relationships with stakeholders in the viewpoints hierarchy, C&A process goals in the goal hierarchy, and risk factors in the risk assessment taxonomy [18].

Questionnaires have also been developed for determining a complete and justifiable set of applicable security requirements for the target system [21]. Well-defined answer options prune the hierarchical requirements domain model categories and establish criteria for requirements applicability.

4.3 Evidence Gathering

C&A activities are all about collecting supporting evidences from the target system to assess the level of compliance with C&A requirements. However, no uniform representation format exists to collect such evidences. As a result, the C&A activities often resort to ad-hoc test procedures and subjective judgments to establish compliance with C&A requirements.

To address these issues, for each C&A requirement the PDO development involves the creation of structured compliance questionnaires by a subject matter 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 evaluate a C&A requirement [21].

This leads to another key design objective for the C&A workbench, which is to use the C&A requirements for providing a context for systematically gathering and analyzing evidences of secure software assurance from the target system. The requirements compliance questionnaires and chosen answer options will drive interactive interfaces to elicit appropriate evidences from the stakeholders.

4.4 Security Risk Assessment

Software security certification approaches adopt a risk-based/aware strategy to provide cost-effective recommendations. Also, in [23], the need for integrating risk analysis into the security requirements engineering process has been strongly suggested. As a result, risk assessment activities to identify the value of the system assets, threats, vulnerabilities, and countermeasures are interleaved throughout the C&A process. However, from our experience with DITSCAP [5] and the study of other risk assessment approaches such as OCTAVE^{SM} [1], we observe that risk assessment approaches lack specific guidelines to utilize the evidences gathered for C&A requirements for performing security risk assessment. These approaches rely on knowledge from experts, users, and past experiences/ records to perceive potential risks, but lack a systematic baseline for identifying risks in a socio-technical environment unique to the organization. To this end, we identify that certification requirements implicitly embed notions of risk components (assets, threats, vulnerabilities, and countermeasures) based on organizational concern for risks most critical in their environment. However, due to lack of structure in natural language C&A requirements specifications (with often missing pieces of information) their compliance evidences are hard to utilize systematically during risk assessment.

These issues suggest another key design objective of supporting requirements-driven security risk assessment in the C&A workbench. Towards this objective, for each certification requirement, the PDO explicitly identifies the risk components that are most critical to software systems deployed in a given distinctive socio-technical environment of the organization. Specifically, within the PDO we capture the interdependencies that exist among C&A requirements in the Requirements Domain Model, and risk components in Domain-specific Taxonomies of Threats, Assets, Countermeasures, and Vulnerabilities [16]. We have extended the Common Criteria security model [3] to incorporate security requirements and its relationships with the risk components.

Examining evidences for an individual C&A requirement does not guarantee overall system dependability; unless, these evidences are put into the context of the target system operational environment along with evidences gathered for other relevant C&A requirements. Therefore, in the operational context of the target system, we have applied Formal Concept Analysis (FCA) [10] to represent and systematically reason about arbitrary relationships between C&A requirements and risk factors modeled in the PDO [9].

4.5 C&A Documentation, Reporting and Visualization

C&A activities involve extensive documentation. DITSCAP follows a single document approach and mandates recording all activities within the System Security Authorization Agreement (SSAA). However, it is entirely up to the discretion of the certification analyst to document and manage system security activities. A lack of standardization in documentation and terminology does not allow C&A documentation to be easily compared or analyzed across multiple system environments [30].

To address these issues, we suggest a C&A requirements-centric approach to collect (using structured questionnaires) and assemble system documentation in the C&A workbench. Based on our approach, the information gathered about the target information system through the requirements compliance questionnaires can be transformed into the required form of documentation for reuse across multiple software assurance initiatives, saving costly rework. In addition, a rich mapping between software artifacts produced throughout the software lifecycle and relevant certification requirements will allow a systematic and context rich retrieval of evidences to support C&A decisions.

The sheer volume of information contained in C&A documentation is often overwhelming, making it less useful in contributing to meaningful conclusions or decisions. To overcome this problem, the PDO also provides ample opportunities within the C&A workbench for visual analytics [29] and reporting at different levels of abstraction to diverse stakeholders.

5. C&A Workbench Architecture

Based on the design objectives identified in the previous section, it is obvious that a C&A workbench requires integrating various components/tools that assist/automate C&A process activities. However, tight coupling of a C&A workbench with a given process definition, leads to poor adaptability when the format of required C&A artifacts or process activities evolve/change. To address these issues, we now discuss a C&A workbench architecture that leverages a unique combination of service and aspect-oriented design paradigms.

4.1 C&A Knowledge Services

The C&A requirements and related domain concepts modeled in the PDO are fundamental to C&A activities supported through the designed workbench. Therefore, we build specialized service facades upon on the OKBC compliant [2] APIs offered by the GenOM knowledge-base [15] to define *C&A knowledge services* for common operations on a specific knowledge model (for e.g. the requirements domain model) in the PDO. The common operations on a knowledge model include editing, browsing, accessing, querying, inferring, and visualization. Each C&A process support component/tool in the workbench consumes a combination of C&A knowledge services to achieve the goals of the associated C&A activity. An overview of knowledge services is shown in Figure 4 as part of the overall conceptual workbench architecture.

4.2 Process Guidance Knowledge Service

The workbench architecture needs to be flexible enough to allow the C&A process definition to evolve independent of the components/tools and services that assist process activities. Therefore, to reduce the impact of C&A process variability on the workbench architecture, we move towards an ontological definition of the workbench supported process activities. The ontological process model is exposed as a knowledge service that guides the composition of C&A process support components/tools and C&A knowledge services for dynamically establishing a workflow in the C&A workbench. It also addresses the needs to tailor the C&A process to a particular level of certification rigor and the unique characteristics of each target system and/or application domain.

From a theoretical perspective the ontological process definition, which we call as a *Process Aspect* [8], supports early separation of the process-related crosscutting concerns that are later dynamically woven into the workbench architecture.

To create a DITSCAP process aspect, as a first step, we identify the core process workflow components that are applicable across all types of target systems as shown in Figure 1.

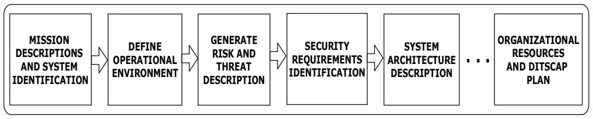

MISSION DESCRIPTIONS AND SYSTEM IDENTIFICATION
DEFINE OPERATIONAL ENVIRONMENT
GENERATE RISK AND THREAT DESCRIPTION
SECURITY REQUIREMENTS IDENTIFICATION
SYSTEM ARCHITECTURE DESCRIPTION
. . .
ORGANIZATIONAL RESOURCES AND DITSCAP PLAN

Figure 1: The DITSCAP Workflow Components

The second step involves a goal-driven decomposition of each workflow component in Figure 1 to specific activities that satisfy their higher level workflow goals. Also, for each activity we identify the required artifacts from the DITSCAP application manual [5] and subject matter experts. As an example, goal-driven workflow component operationalization of the "Generate Risk and Threat Description" DITSCAP workflow component is shown in Figure 2. The resulting model, abstracts the interactions between the core process workflows components and the software components/tools that support corresponding C&A activities in those workflow components.

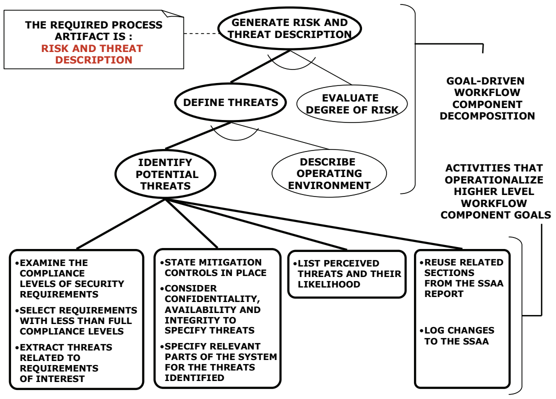

THE REQUIRED PROCESS ARTIFACT IS : RISK AND THREAT DESCRIPTION
GENERATE RISK AND THREAT DESCRIPTION
DEFINE THREATS
EVALUATE DEGREE OF RISK
IDENTIFY POTENTIAL THREATS
DESCRIBE OPERATING ENVIRONMENT
GOAL-DRIVEN WORKFLOW COMPONENT DECOMPOSITION
ACTIVITIES THAT OPERATIONALIZE HIGHER LEVEL WORKFLOW COMPONENT GOALS
•EXAMINE THE COMPLIANCE LEVELS OF SECURITY REQUIREMENTS
•SELECT REQUIREMENTS WITH LESS THAN FULL COMPLIANCE LEVELS
•EXTRACT THREATS RELATED TO REQUIREMENTS OF INTEREST
•STATE MITIGATION CONTROLS IN PLACE
•CONSIDER CONFIDENTIALITY, AVAILABILITY AND INTEGRITY TO SPECIFY THREATS
•SPECIFY RELEVANT PARTS OF THE SYSTEM FOR THE THREATS IDENTIFIED
•LIST PERCEIVED THREATS AND THEIR LIKELIHOOD
•REUSE RELATED SECTIONS FROM THE SSAA REPORT
•LOG CHANGES TO THE SSAA

Figure 2: Goal-driven Workflow Component Operationalization

The process aspect also abstracts the interactions between the software components/tools (as thick client-side interfaces) and the combination of C&A knowledge services they consume to achieve the goals of the corresponding C&A activity. Capturing these interactions requires a mapping of the functions supported by software components/tools to appropriate operations provided by C&A knowledge services. Specifically, the process aspect ontology models these interactions as process composition rules that fire at particular points in the workflow execution. These rules enable many to many interactions, promoting reuse of software components/tools and knowledge services. Figure 3 shows such interactions for the "Security Requirements Identification" DITSCAP workflow component.

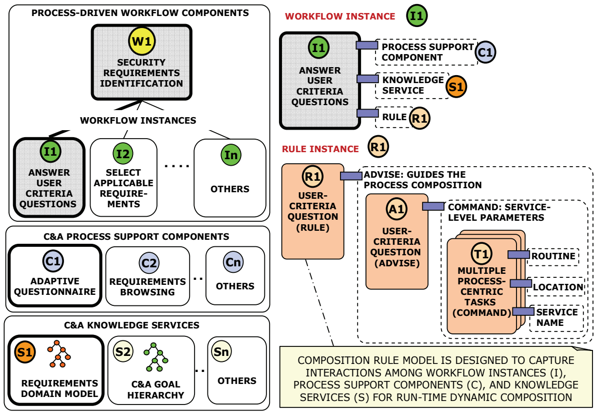

PROCESS-DRIVEN WORKFLOW COMPONENTS
W1
SECURITY REQUIREMENTS IDENTIFICATION
WORKFLOW INSTANCES
I1
ANSWER USER CRITERIA QUESTIONS
I2
SELECT APPLICABLE REQUIRE-MENTS
In
OTHERS
C&A PROCESS SUPPORT COMPONENTS
C1
ADAPTIVE QUESTIONNAIRE
C2
REQUIREMENTS BROWSING
Cn
OTHERS
C&A KNOWLEDGE SERVICES
S1
REQUIREMENTS DOMAIN MODEL
S2
C&A GOAL HIERARCHY
Sn
OTHERS
WORKFLOW INSTANCE I1
I1
ANSWER USER CRITERIA QUESTIONS
PROCESS SUPPORT COMPONENT C1
KNOWLEDGE SERVICE S1
RULE R1
RULE INSTANCE R1
R1
USER-CRITERIA QUESTION (RULE)
ADVISE: GUIDES THE PROCESS COMPOSITION
A1
USER-CRITERIA QUESTION (ADVISE)
COMMAND: SERVICE-LEVEL PARAMETERS
T1
MULTIPLE PROCESS-CENTRIC TASKS (COMMAND)
ROUTINE
LOCATION
SERVICE NAME
COMPOSITION RULE MODEL IS DESIGNED TO CAPTURE INTERACTIONS AMONG WORKFLOW INSTANCES (I), PROCESS SUPPORT COMPONENTS (C), AND KNOWLEDGE SERVICES (S) FOR RUN-TIME DYNAMIC COMPOSITION

Figure 3: Interactions Captured by Process Aspect

While using GenOM to model the process aspect, a specialized service facade exposes the process aspect as a *process guidance knowledge service* to dynamically compose the C&A workbench architecture. Dynamic composition of the architecture refers to assembling the C&A knowledge services and the components/tools which utilize the functionality exposed through these services for executing the C&A process workflow.

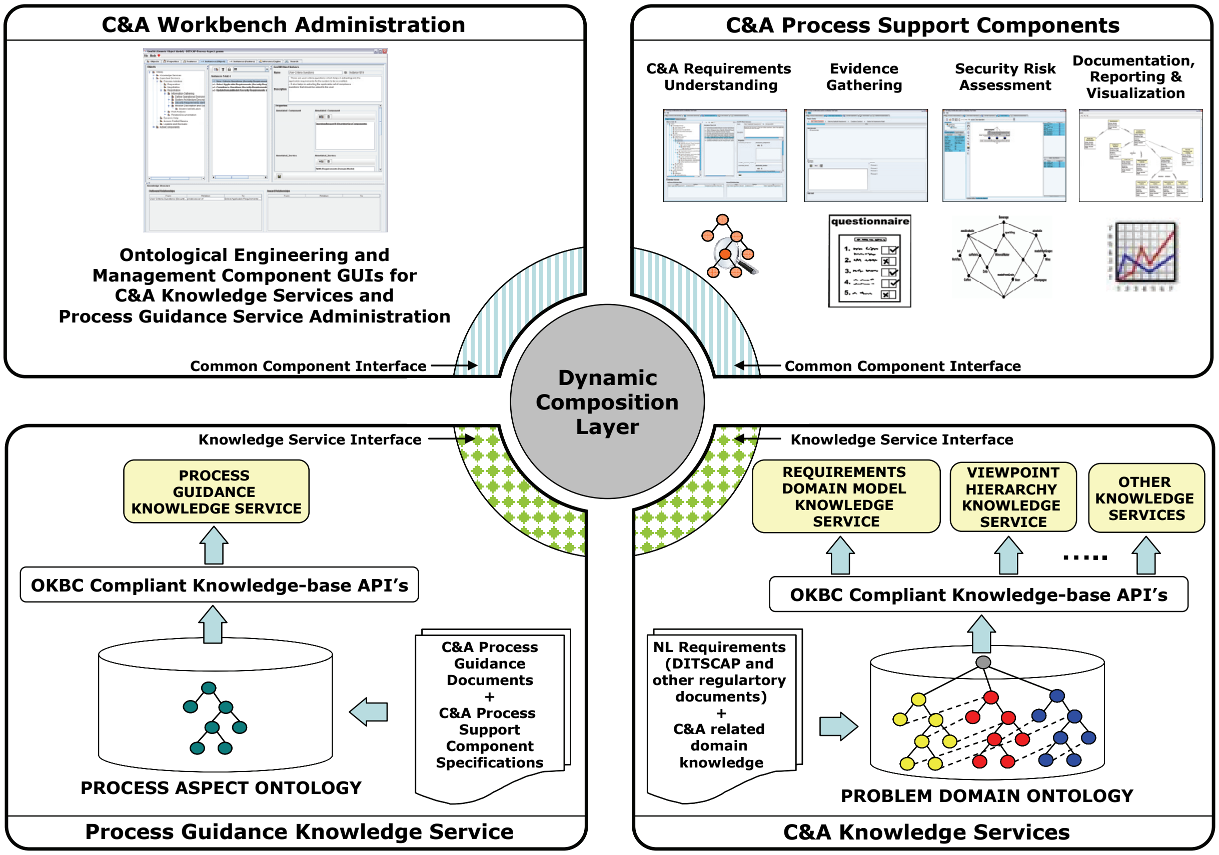
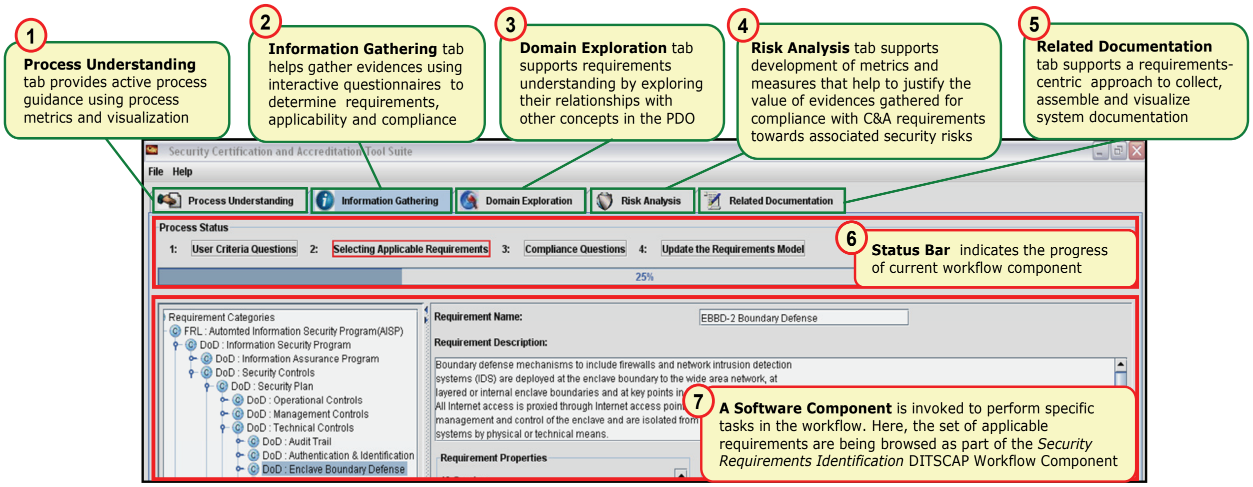

C&A Workbench Administration
Ontological Engineering and Management Component GUIs for C&A Knowledge Services and Process Guidance Service Administration
Common Component Interface
C&A Process Support Components
C&A Requirements Understanding
Evidence Gathering
Security Risk Assessment
Documentation, Reporting & Visualization
questionnaire
Common Component Interface
Dynamic Composition Layer
Knowledge Service Interface
PROCESS GUIDANCE KNOWLEDGE SERVICE
OKBC Compliant Knowledge-base API's
PROCESS ASPECT ONTOLOGY
C&A Process Guidance Documents + C&A Process Support Component Specifications
Process Guidance Knowledge Service
Knowledge Service Interface
REQUIREMENTS DOMAIN MODEL KNOWLEDGE SERVICE
VIEWPOINT HIERARCHY KNOWLEDGE SERVICE
.....
OTHER KNOWLEDGE SERVICES
OKBC Compliant Knowledge-base API's
NL Requirements (DITSCAP and other regulartory documents) + C&A related domain knowledge
PROBLEM DOMAIN ONTOLOGY
C&A Knowledge Services

Figure 4: C&A Workbench Conceptual Architecture

4.3 Conceptual Workbench Architecture

A conceptual architecture for the C&A workbench is shown in Figure 4. The *Dynamic Composition Layer* is responsible for integrating the C&A workflow as defined by the *process guidance knowledge service*. The C&A knowledge services are consumed by the C&A process support components based on this guidance. The C&A workbench conceptual architecture in Figure 4 has been used for designing a prototype system to support the DITSCAP. A process composition algorithm is implemented, as part of the dynamic composition layer shown in Figure 4. A well-annotated screenshot, as shown in Figure 5, identifies key features of the implemented prototype system. Different tabs in the prototype system seek to realize the design objectives outlined in section 4.



1 **Process Understanding** tab provides active process guidance using process metrics and visualization

2 **Information Gathering** tab helps gather evidences using interactive questionnaires to determine requirements, applicability and compliance

3 **Domain Exploration** tab supports requirements understanding by exploring their relationships with other concepts in the PDO

4 **Risk Analysis** tab supports development of metrics and measures that help to justify the value of evidences gathered for compliance with C&A requirements towards associated security risks

5 **Related Documentation** tab supports a requirements-centric approach to collect, assemble and visualize system documentation

Process Status

1: User Criteria Questions 2: Selecting Applicable Requirements 3: Compliance Questions 4: Update the Requirements Model

25%

6 **Status Bar** indicates the progress of current workflow component

Requirement Categories
- FRL : Automted Information Security Program(AISP)
  - DoD : Information Security Program
    - DoD : Information Assurance Program
    - DoD : Security Controls
      - DoD : Security Plan
        - DoD : Operational Controls
        - DoD : Management Controls
        - DoD : Technical Controls
          - DoD : Audit Trail
          - DoD : Authentication & Identification
          - DoD : Enclave Boundary Defense

Requirement Name: EBBD-2 Boundary Defense

Requirement 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
All Internet access is proxied through Internet access poin
management and control of the enclave and are isolated from
systems by physical or technical means.

Requirement Properties

7 **A Software Component** is invoked to perform specific tasks in the workflow. Here, the set of applicable requirements are being browsed as part of the *Security Requirements Identification* DITSCAP Workflow Component

Figure 5: A Screenshot of the C&A Workbench Prototype Implementation

6. Contributions and Future Work

The ultimate goal of software certification is to promote assurance among stakeholders. Therefore, we claim that all C&A activities and their results are understood effectively only when grounded in the context of (and traceable to) C&A requirements from multiple dimensions in the problem domain. Thus, a common understanding of certification requirements and related domain concepts is critical.

In this paper we characterize the nature of C&A requirements and associated problems based on our experience with DITSCAP, while pointing out the shortcomings of the current C&A approaches. Such understanding is critical to design a requirements-driven C&A workbench. Towards this goal, we identify potential solutions based on our on-going research activities and outline how they can contribute to an integrated C&A workbench. We also outline a flexible and dynamic architecture to support maximum reuse of available knowledge resources and tools in the C&A workbench.

As we move from platform-specific architectures towards net-centricity, sharing and reuse of C&A artifacts, supporting tools, requirements models, and domain knowledge is critical. The architecture of the C&A workbench outlined in this paper enables us to leverage the flexibility of service and aspect-oriented design paradigms to move towards such a future computing paradigm. In addition, a step-wise (and flexible) evolution of the C&A workbench will help to identify the effectiveness of our approach on the artifacts resulting from C&A activities.

7. References

[1] Alberts, C. and Dorofee, A. "OCTAVE^{SM} Criteria, Version 2.0", CMU/SEI-2001-TR-016 December 2001.

[2] Chaudhri, V. K., Farquhar, et al, "OKBC: a programmatic foundation for knowledge base interoperability," In Proc. 15th Nat. Conf. on Artificial intelligence, AAAI, USA, pp: 600-607, 1998.

[3] Common Criteria, Introduction and general model. Ver. 2.1. ISO/IEC 15408-1, 1999

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

[5] DoD 8510.1-M, "DITSCAP Application Manual," 2000.

[6] DoD Instruction 5200.40: DITSCAP, 1997.

[7] Ernst & Young, "Report on the Widening Gap," 8th Annual Global Information Security Survey, Netherlands, 2005.

[8] Gandhi, R. A., Siddharth, W., and Lee, S.W., "Process Artifacts Defined as an Aspectual Service to System Models," In Proc. of the 2nd Int'l Workshop on Service-Oriented Computing: Consequences for Engineering Requirements (SOCCER'06), at the 14th Int'l Requirements Engg. Conf. (RE'06), MN, USA, 2006.

[9] Gandhi, R.A. and Lee, S.W., "Understanding Risks in an Organizational Infrastructure during Software Certification Activities," TR: SIS-NISE-07-01, UNC Charlotte, NC, 2007

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

[11] GAO, Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements, GAO-05-552, Washington, D.C., July 15, 2005.

[12] I-Assure, LLC., autoRTM, 2005 <http://www.i-assure.com>

[13] Lee, S.W., Gandhi, R.A, et al., "Building problem domain ontology from security requirements in regulatory documents," In Proc. 2nd Int'l Workshop on Software Engineering For Secure Systems (SESS 06), ACM Press, New York, NY, 2006 pp. 43-50.

[14] Lee, S.W. Gandhi, R. A. "Engineering Dependability Requirements for Software-intensive Systems through the Definition of a Common Language," In Proc. Workshop on Requirements Engg. for High-Availability Systems (RHAS), at 13th IEEE Int'l Requirements Engg. Conf. Paris, France, IEEE Press, 2005

[15] Lee, S.W. and Yavagal, D., "GenOM User's Guide," TR: SIS-NISE-04-01, UNC Charlotte.

[16] Lee, S.W., Gandhi, R.A. and Ahn, G., "Security Requirements Driven Risk Assessment for Critical Infrastructure Information Systems", In Proc. Symposium on Requirements Engg. for Information Security (SREIS'05), at 13th IEEE Int'l Requirements Engg. Conf. (RE '05), Paris, France, IEEE Press, 2005

[17] Lee, S.W. and 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.

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

[19] Lee, S.W., Gandhi, R.A., Ahn, G., "Establishing Trustworthiness in Services of the Critical Infrastructure: Automating the DITSCAP. In Proc. 1st Workshop on Software Engg for Secure Systems (SESS 05), at 27th IEEE Int'l Conf. on Software Engg. (ICSE'05), St. Louis, MO, USA, 2005, pp. 43-49

[20] Lee, S.W., Gandhi, R.A., Ahn, G.J., "Certification Process Artifacts Defined as Measurable Units for Software Assurance," International Journal on Software Process: Improvement and Practice (April, 2007), Online-Early View is published & available on Dec 2006 through Wiley InterScience: DOI:10.1002/spip.313

[21] Lee, S.W., Muthurajan, D., Gandhi, R.A., et al., "Building decision support problem domain ontology from natural language requirements for software assurance," International Journal on Software Engineering and Knowledge Engineering, Vol. 16, No.6, pp.1-34, December, World Scientific, 2006.

[22] McGuinness, D., van Harmelen, F. (eds), "OWL Web Ontology Language Overview", W3C Recommendation, 2004

[23] Moffett, J. D., Haley, C. B., Nuseibeh, B.A, "Core Security Requirements Artefacts," Technical Report 2004/23, Milton Keynes, UK: Department of Computing, The Open University, June 2004

[24] Office of Management and Budget (OMB), "FY 2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002," March 1, 2006

[25] SecureInfo, Compliance Authority (built on RMS technology), 2005, <http://www.secureinfo.com/>

[26] Swartout, W., Tate, A., "Ontologies," IEEE Intelligent Systems, 14(1), 1999, pp: 18-19

[27] The United States General Accounting Office, "Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation," Report to Congressional Requestors, GAO-04-376

[28] The United States General Accounting Office, "Department of Homeland Security Needs to Fully Implement its Security Program," Report to Congressional Requestors, GAO-05-700

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

[30] Turner, G., Holley, et al., "Net-Centric Assured Information Sharing – Moving Security to the Edge through dynamic C&A," IANewsletter, Vol.8(3), Winter 2005/2006

[31] van Lamsweerde, A., "Goal-Oriented Requirements Engineering: A Roundtrip from Research to Practice," In Proc. 12th IEEE Int'l Requirements Engg Conference, Kyoto, 2004, pp. 4-8.

[32] Xacta Corporation, Xacta IA Manager, 2004 <http://www.xacta.com/>