Requirements as Enablers for Software Assurance

Dr. Seok-Won Lee and Robin A. Gandhi
The University of North Carolina at Charlotte

The level of compliance with Certification and Accreditation (C&A) requirements conveys the level of assurance that one can expect from the quality of software behavior. Therefore, it is critical to understand the C&A requirements in terms of their applicability, scope, and impact of non-compliance on diverse aspects of software behavior to justify its certified qualities. However, numerous C&A requirements in ambiguous natural language descriptions with different levels of granularity are scattered across multiple documents that are used as guidance for C&A activities. As a result, a great deal of subjectivity is involved in understanding C&A requirements and their evaluation. This article discusses our approach to represent, model, and analyze C&A requirements to promote a common understanding among stakeholders for engineering more reliable software.

The Department of Defense (DoD) increasingly relies on the Defense Information Infrastructure (DII) that connects mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and provides information processing and other value-added services [1]. These services are dependent on the quality of underlying software, systems, practice, and environment to promote trust in the information furnished to the DoD and national-level decision makers. Therefore, the infrastructure-wide DoD Information Technology Security Certification and Accreditation Process (DITSCAP) [1] was introduced to ensure that the DoD's needs for software assurance are uniformly considered and maintained throughout the life cycle of all information systems that support information processing services within the DII.

The DITSCAP[1] is the standard DoD process for identifying information security requirements, providing security solutions and managing information systems security activities [1]. DITSCAP defines certification as the comprehensive evaluation of the technical and non-technical security features of an information system to establish the extent to which a particular design and implementation meets a set of specified security requirements. After this evaluation, the accreditation statement is an approval to operate the information system in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. Using the DITSCAP to certify an information system is not simply a one-time process; it is maintained throughout the life cycle of the information system.

DITSCAP Limitations

Security requirements for DITSCAP certification address software assurance needs from diverse dimensions of process, organization, cost, time, data sensitivity, user clearance, system capabilities, development, deployment, maintenance, architecture, inventory, impact of non-availability, operational facilities, and other socio-technical aspects. Despite such a comprehensive coverage of software assurance needs, current DITSCAP practices have several limitations.

Practicing DITSCAP requires familiarity with several guidance documents from different levels in the DoD organizational hierarchy to identify the applicable set of security requirements necessary for certification. These documents include the DITSCAP application manual [2]; federal laws from the Office of Management and Budget; public laws; DoD and Department of Navy (DoN)[2] information assurance policies and implementations; National Institute of Standards and Technology (NIST) best practices for computer security; and many others. Each document usually ranges between 25 and 200 pages with heavy cross-referencing to other documents, making it extremely difficult to manually comprehend the interdependencies among their contents. In essence, the certification requirements with different levels of granularity in their specifications are scattered across multiple documents that provide guidance for C&A activities. These factors introduce a great deal of subjectivity in making decisions about the applicability, scope, and impact of non-compliance of DITSCAP security requirements. Table 1 summarizes these key decision points. Addressing these decision points with objective, justifiable, and repeatable criteria is critical to establish the assurance of reliable behavior of an information system subject to DITSCAP certification requirements. However, the interdependencies that exist among numerous certification requirements from multiple sources/documents severely complicate these decision points.

Due to the non-functional nature of DITSCAP certification requirements, these requirements often constrain diverse aspects of information system behavior in complex ways that are not readily apparent from their natural language descriptions. Additionally, understanding the interactions among various aspects of information system behavior is essential to reveal the cascading effects of the impact from the non-compliance of a certain certification requirement on overall system dependability.

Due to the limitation of current practices in addressing these issues, justifying compliance with certification requirements often satisfies a mere bureaucratic necessity without thoroughly understanding their consequences on the overall information system dependability and associated security risks. As a result, despite enormous efforts and resources currently spent on DoD software assurance initiatives, their effectiveness is only limited [3].

The Need for a Common Understanding of Requirements

Natural language security requirements for DITSCAP certification have little or no structural regularity in their specifications. Based on the seven facets of *complete* requirements – *who*, *where*, *what*, *when*, *why*, *which,* and *how* – a security requirement typically requires one to identify concepts related to 1) the assets that it protects, 2) the threats that it is driven by, 3) the vulnerabilities that it prevents, 4) the countermeasures that it suggests, 5) the mission criticality that it is subject to, 6) its source, 7) the goal of the security requirement, 8) the related stakeholders, and 9) other domain-specific concepts that need to be considered for creating a context that facilitates their uniform interpretation. However, most DITSCAP-enforced security requirements either do

not explicitly identify these concepts or they are dispersed across multiple documents, making it difficult to practice DITSCAP and utilize its results for promoting software assurance.

To address these issues, we focus our research efforts on understanding and modeling the DITSCAP security requirements and related concepts in ways that support software assurance efforts. It is important to recognize that the assurance of trustworthy software behavior is determined by the needs of the problem domain. For example, in the DoD problem domain, security is of primary concern, whereas in the aviation problem domain, safety is of primary concern. Therefore, to effectively understand software assurance needs in the DoD as scoped by DITSCAP security requirements, we have produced a DITSCAP problem domain ontology. The meaning of ontology as adopted from the field of knowledge engineering refers to a set of concepts or terms that can be used to describe some area of knowledge or build a representation of it.

By combining techniques from requirements engineering and knowledge engineering we produce hierarchical ontological models [4] that characterize software assurance needs of the DoD. Specifically, we analyze each DITSCAP-related guidance document to extract ontological concepts that help in classifying and categorizing the DITSCAP security requirements from diverse dimensions. These ontological concepts are modeled as a hierarchy with several non-taxonomic interdependencies identified from DITSCAP-related guidance documents. The resulting ontology explicitly captures the concepts related to certification requirements and the relationships among them at different levels of granularity, previously scattered across multiple documents. The ontology promotes a common understanding among various stakeholders regarding DITSCAP security requirements specified within the federal, DoD, DoN, and NIST guidance documents at different levels of abstraction. Such a structured representation of DITSCAP security requirements facilitates a uniform understanding of their applicability, scope, and impact of non-compliance through its explicit traceable rationales and visual exploration capabilities.

Our 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) that effectively characterize the required dependable software behavior from diverse dimensions. The resulting integrated ontology is a human and machine understandable, hierarchical model of software assurance needs in the DoD, engineered using object-oriented ontological domain modeling techniques [5]. Goal-, scenario-, and viewpoint-based requirements engineering techniques are used to drive the identification of concepts related to a security requirement from DITSCAP-related guidance documents as structured representations of the following: 1) A hierarchy of requirement types that categorize security requirements from DITSCAP-related guidance documents; 2) A viewpoints hierarchy that models different perspectives and related stakeholders of a security requirement; 3) A risk assessment taxonomy that models risk factors from a broad spectrum of perceived risk sources identified in DITSCAP security requirements; 4) A hierarchy of C&A goals and related scenarios that models the DITSCAP process activities for gathering user/system criteria related to determining the applicability of security requirements; 5) A network-based information discovery taxonomy that aggregates results from network monitoring tools and scripts to assess compliance with security requirements in the actual environment; and 6) Interdependencies among various concepts in the DITSCAP ontology. These ontological concepts classify and categorize the certification requirements from multiple dimensions. Here, we briefly discuss the goal-driven process of identifying interdependent certification requirements categories scattered across multiple documents to produce a requirements hierarchy; however, further details about other models are in [5, 6] or available by contacting the authors.

Decision Point Categories	Key DITSCAP Decision Points
Applicability	DP1. Which regulatory documents should be used to identify C&A requirements? DP2. At what level of granularity should C&A requirements be identified? DP3. What are the types of the systems (for example, a major application or general support system) addressed by C&A requirements? DP4. What redundancies exist among C&A requirements and how should they be discovered?
Scope	DP5. Is the identified set of applicable C&A requirements complete? DP6. Who is responsible for or affected by (stakeholders) the C&A requirements?
Impact of Non-compliance	DP7. What are the criteria to assess requirements compliance? DP8. Do the compliance criteria provide a complete coverage of the different dimensions addressed by a given requirements? DP9. What are the risks associated with the system at a particular compliance level with C&A requirements?

Table 1: *DITSCAP Decision Points*

Requirements Extraction and Modeling

As a first step towards understanding DoD software assurance needs based on DITSCAP security requirements, we identify the interdependencies among DITSCAP-related guidance documents using the cross-referential nature of their contents. We determine a hierarchical relationship among the generic federal-level documents, domain-spanning DoD and DoN policy/NIST security guidance documents, and site/agency specific DoD and DoN information assurance implementation guidance documents based on the level of abstraction pertaining to DITSCAP certification requirements specified within them.

Once the document interdependencies become apparent, a top-down goal decomposition approach systematically identifies interdependent requirements categories from multiple documents at different levels of abstraction. High-level assurance goals identified from certification requirements in federal-level guidance documents drive the elicitation of specific certification requirements which satisfy their parent goals from DoD/DoN/NIST guidance documents. Figure 1 (see page 22) elaborates on this process for the high-level assurance goal of *Screening Individuals* identified from certification requirements (annotated using the Label

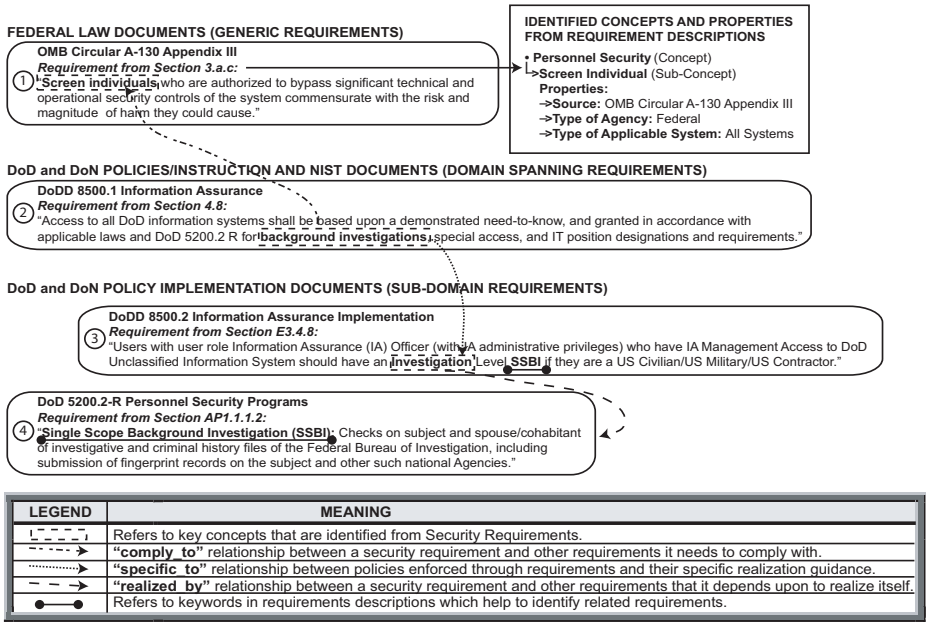
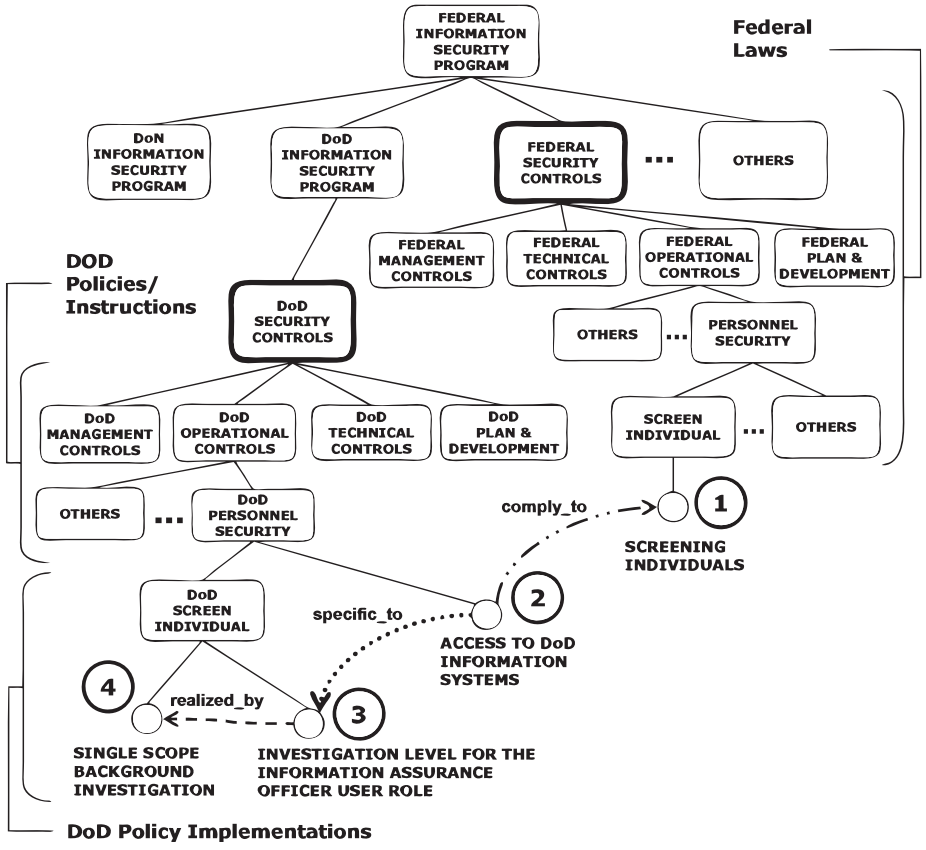


Figure 1: *Extraction of Security Requirements, Categories, Properties, and Their Interdependencies From DITSCAP-Related Guidance Documents*

1) expressed in a federal-level document. To satisfy this goal, we identify specific certification requirements pertaining to *background investigation* and other relevant security requirements categories (annotated using the Labels 2, 3, and 4 in Figure 1) from DoD/DoN/NIST documents. This process explicitly models the security requirement categories, their properties, and the relationships among them, spanning multiple DITSCAP-related guidance documents from different levels in the DoD organizational hierarchy.

The requirements hierarchy, modeled within the DITSCAP ontology, aggregates these requirements categories through a hierarchical representation that includes top-level generic requirements categories, mid-level domain spanning requirements and low-level agency specific requirements. Such a hierarchical organization of requirements types allows for a systematic exploration of DITSCAP security requirements during certification activities. A partial requirements hierarchy that explicitly models the requirements categories and their relationships identified in Figure 1 is depicted in Figure 2 with corresponding requirement labels. The security requirements hierarchy also promotes consistency in managing requirements from multiple documents by providing a generic set of categories. For example in Figure 2, the *Federal Security Controls* and *DoD Security Controls* requirements categories provide consistency and traceability among certification requirements extracted from federal and DoD C&A guidance documents respectively.

Figure 2: *A Partial Requirements Hierarchy*



Metrics and Measures for Compliance With Certification Requirements

For each certification requirement modeled within the requirements hierarchy, the DITSCAP ontology development also involves the creation of compliance questionnaires (representative of various compliance metrics) with well-defined answer options (representative of compliance measures). These questionnaires systematically gather evidences for the target information system to determine its eligibility for DITSCAP certification. Utilizing DITSCAP-related guidance documents and domain expertise, we establish the criteria addressed by questionnaires. Responses to these questionnaires are gathered by consulting various sources related to the target information system such as users, operating manuals, plans, architecture diagrams, or through network monitoring tools and scripts. These responses establish the extent to which the higher-level requirements categories in the requirements hierarchy are satisfied through specific policies, procedures, or technical rationales in the actual environ-

Our ontology development efforts are supported by the GENeric Object Model (GenOM) toolkit [7]. GenOM is an integrated development environment (developed at the University of North Carolina - Charlotte [UNCC] and available for use) for ontological engineering processes with functionalities to create, browse, access, query, and visualize associated ontologies. GenOM is compatible with the Web Ontology Language representation [8] and is associated with an inference engine that supports reasoning upon the ontological concepts and relationships modeled in its knowledge bases.

ment. The questionnaires introduce uniformity in the evaluation of security requirements while avoiding subjective interpretations of certification requirements compliance criteria.

The compliance information gathered for DITSCAP certification requirements can also be interpreted in terms of other models within the DITSCAP ontology. The natural language descriptions of DITSCAP security requirements embody concepts which help in establishing these relationships. From requirements descriptions we identify concepts related to stakeholders in the viewpoints hierarchy; C&A process goals in the goal hierarchy; risk factors of threat, vulnerabilities, countermeasures, assets, and mission criticality in the risk assessment taxonomy; and actual system characteristics captured through the network-based information discovery taxonomy. Such relationships for the DITSCAP certification requirement of *Enclave Boundary Defense* with other concepts within the DITSCAP ontology are visualized in Figure 3. Such explicitly modeled relationships have also helped in perceiving the operational risks based on the level of compliance of the target information system with DITSCAP security requirements [9].

Benefits of Our Approach

Our approach for DITSCAP security requirements modeling and analysis has many of the following potential benefits:

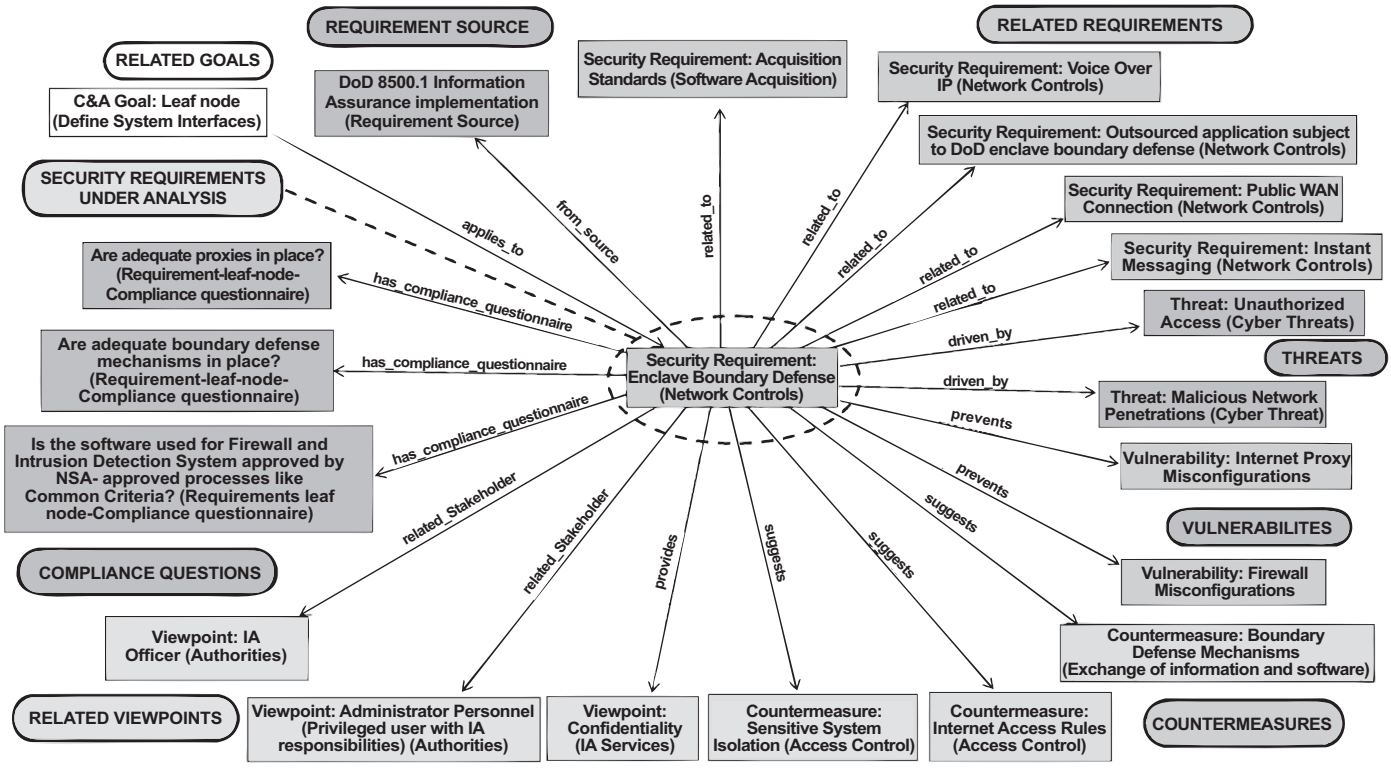
- A reusable and configurable repository of certification requirements, policies, and directives. This gives users the ability to map and reflect the appropriate language of existing requirements applicable to their agency.
- Intuitive Graphical User Interfaces can be supported through the DITSCAP ontology to guide C&A process activities.
- Currently, no systematic methods exist to collect information related to the compliance level of certification requirements. Additionally, a long and exhaustive task of gathering requirement compliance criteria from the target system results in a subjective and ad-hoc C&A process. To address these issues, an ontology-driven methodology to gather compliance information using well-defined questionnaires (metrics and measures) for certification requirements provides objective and uniform criteria to facilitate cost-effective decision making.
- 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.
- The hierarchical representation of DITSCAP ontology provides the flexibility of communicating compliance results at different levels in the organization and sharing them among agencies based on a common understanding.
- Reducing the certification costs due to the need of fewer resources to conduct, manage, and maintain C&A activities. Efficient C&A activities can significantly reduce the development and deployment time of more reliable information systems.

Current Status, Challenges and Next Steps

Through our efforts, a prototype DITSCAP automation tool has been developed. We are currently in the process of outlining a case study designed research methodology where a group of experts perform C&A activities with and without using the DITSCAP ontology and related tool support. The results of this case study with evaluation metrics and measures will eventually serve as a basis for establishing the benefits of our approach.

We realize that based on the given target information system, it is essential to discover *links* among non-functional certification requirements which may originate from different dimensions, but are necessary to collectively ascertain overall reliable emergent software behavior. Although such links cannot be anticipated or formalized for all situations, we will explore ways to utilize the traceability offered within the DITSCAP ontology to help experts gradually hypothesize more meaningful relationships among

Figure 3: *Visualization of a DITSCAP Security Requirement and Its Relationships With Other Concepts*



non-functional certification requirements while understanding their consequences on the overall dependable behavior of the target information system.

Due to the nature of the ontological engineering, currently the DITSCAP ontology has been constructed manually using frequent feedback and refinement from experts. We also explore techniques for automatically processing natural language guidance documents and identify ontological concepts that experts can refine further.

Reaching Out

In general, our approach helps in capturing the characteristics of information present sparsely in documents and the way these characteristics can be represented using ontological modeling processes to infer valuable knowledge that assists decision making activities. Hence, we contend that our methodology can be favorably extended to non-DITSCAP uses (e.g. Federal Information Security Management Act, NIST, Common Criteria, or the Health Insurance Portability and Accountability Act) where the decision making activities require sifting through large volumes of information.

Our research efforts seamlessly complement the migration from DITSCAP to DoD Information Assurance Certification and Accreditation Process (DIACAP) for future DoD endeavors of the Global Information Grid and net-centric dynamic C&A [10]. The DIACAP Enterprise Mission Assurance Support System that standardizes approaches for describing and collecting data for C&A can leverage the benefits of an ontological representation of security requirements to promote uniformity, reusability, and portability, as well as the sharing of results from C&A activities. The DITSCAP ontology also facilitates the interpretation of results from network monitoring tools and scripts in terms of their impact to compliance with certification requirements, providing interesting research directions for the DIACAP Vulnerability Assessment Management Service.◆

Acknowledgement

This work is partially supported by the grant from the Critical Infrastructure Protection Center, Space and Naval Warfare Systems Center, Charleston, South Carolina.

References

1. DoD. "DoD 5200.40. DITSCAP." Dec. 1997 <www.dtic.mil/whs/directives/corres/html/520040.htm>.
2. DoD. "DoD 8510.1-M, DITSCAP." Application Manual. 2000 <www.dtic.mil/whs/directives/corres/html/85101m.htm>.
3. Davis, T. "No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecard." Press Release. Government Reform Committee, 2005 <http://reform.house.gov/UploadedFiles/TMDFISMA06Opener.pdf> .
4. Swartout, W. and A. Tate. "Ontologies." IEEE Intelligent Systems 141. (1999): 18-19.
5. Lee, S., D. Muthurajan, and R. A. Gandhi, et al. "Building Decision Support Problem Domain Ontology From Natural Language Requirements for Software Assurance." International Journal on Software Engineering and Knowledge Engineering (2006).
6. Lee, S.W., R.A. Gandhi, and Gail-Joon Ahn. "Certification Process Artifacts Defined as Measurable Units for Software Assurance." International Journal on Software Process: Improvement and Practice (2006).
7. Lee, S.W., and D. Yavagal. "GenOM User's Guide Vers. 2.0." Technical Report TR-NiSE-05-05. Knowledge Intensive Software Engineering Research Group. Dept. of Software and Information Systems: UNCC, 2005.
8. McGuinness, D., and F. van Harmelen, Eds. "OWL Web Ontology Language Overview." W3C Recommendation, 2004 <www.w3.org/TR/owl-features/>.
9. Lee, S.W., R.A. Gandhi, and G.J. Ahn. "Security Requirements Driven Risk Assessment for Critical Infrastructure Information Systems." Proc. of the Symposium on Requirements Engineering for Information Security (SREIS 05), 2005.
10. Turner, G., P. Holley, E.J. Mehan, and M. Colon. "Net-Centric Assured Information Sharing – Moving Security to the Edge Through Dynamic Certification and Accreditation." IA Newsletter 8.3 (Winter 2005/2006).

Notes

1. DITSCAP is currently undergoing a migration to the DoDI 8510.bb, DIACAP. However, it does not affect the utility of the approaches outlined in this article.
2. Although we address our approach in the context of the DON, our techniques are generally applicable to C&A standards for other agencies.

About the Authors

Seok-Won Lee, Ph.D., is an assistant professor of software and information systems at UNCC. Prior to UNCC, he was affiliated with Science Applications International Corporation and the IBM T.J. Watson Research Center. Lee's areas of specializations include software engineering and knowledge engineering with specific expertise in ontology-based requirements engineering, knowledge acquisition, and machine learning. Lee is currently focusing on new research in the areas of knowledge-intensive software engineering, software evaluation research, object-oriented domain modeling and their applications to information security and assurance. He holds a master's degree in computer science from the University of Pittsburgh and a doctorate in information technology from George Mason University.

Robin Gandhi is pursuing a doctorate in information technology and has been a research assistant in the Department of Software and Information Systems at UNCC since 2003. His research interests include requirements engineering, knowledge-intensive software engineering, and ontology-based object-oriented domain modeling and analysis. Gandhi received his undergraduate degree in electronics engineering from Sardar Patel University, India, and his Master of Science in computer science from UNCC.

Both authors can be reached at:
Department of Software and Information Systems
UNCC
9201 University City BLVD
Charlotte, NC 28223-0001
Phone: (704) 687-8662/8385
Fax: (704) 687-4893
E-mail: seoklee@uncc.edu,
rgandhi@uncc.edu