To appear in Proceedings of the 27th IEEE International Conference on Software Engineering (ICSE 05),
Software Engineering for Secure Systems (SESS 05) Workshop, St. Louis, Missouri, May 15-21, 2005.

Establishing Trustworthiness in Services of the Critical Infrastructure through Certification and Accreditation

Seok Won Lee, Robin A. Gandhi and Gail-Joon Ahn
Department of Software and Information Systems
The University of North Carolina at Charlotte
9201 University City Blvd., Charlotte, NC 28223, USA
{seoklee, rgandhi, gahn}@uncc.edu

ABSTRACT
Trustworthiness in services provided by the Critical Infrastructure (CI) is essentially dependent on the quality of underlying software, systems, practice and environment, as which the software information infrastructures are becoming increasingly a major component of business, industry, government and defense. The level of trustworthiness required from services that are operational in such critical software information infrastructures is often established based on standardized infrastructure-wide evaluation criteria - Certification and Accreditation (C&A) - through the identification of operational risks and the determination of conformance with established security standards and best practices. In order to effectively establish such levels of trustworthiness for services in the CI, we identify the need for a structured and comprehensive C&A framework with appropriate tool support that combines its theoretical and practical aspects. In this paper, we present our efforts in developing such a framework that leverages novel techniques from software requirements engineering and knowledge engineering to support the automation of the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), which is a standard for certifying and accrediting the information networks that support the Defense Information Infrastructure (DII). Through the examples derived from our case study, we further motivate the applicability and appropriateness of our framework.

Categories and Subject Descriptors
D.2.1 [Software Engineering]: Requirements/Specifications – *structured methodologies, tools.*

General Terms
Measurement, Reliability, Security and Standardization.

Keywords
Information Security Requirements Engineering, Information Systems Certification and Accreditation, Critical Infrastructure Protection, Risk Assessment, Ontological Engineering

Software Engineering for Secure Systems – Building Trustworthy Applications (SESS'05), May 15-16, 2005, St. Louis, Missouri, USA.

1. INTRODUCTION
Recent tragic events and ever growing threats to national security amplify the importance of trustworthiness in services that get delivered through the CI, of which the software information infrastructures are becoming increasingly a major component of business, industry, government and defense. Such software information infrastructures require an effective and comprehensive C&A framework to assess their operational risks, optimize their security posture and evaluate their Information Assurance (IA) practices. Despite such necessities, the criteria to establish the level of trustworthiness required in the services made available through these information infrastructures is often confined and restricted to the experts in the domain or those who are familiar with specific operating systems, programming languages and protocols. Infrastructure-wide standardization of C&A processes seek to address this issue, but the gaps that exist between the standards and their interpretation and enforcement in real world practices diminishes the value of such efforts.

The Department of Defense (DoD) increasingly relies on the services made available through the DII, irrespective of their level of classification, to perform a variety of functions and accomplish their missions. The success of these missions is essentially dependent on the quality of underlying software, systems, practice and environment to provide high quality of service and trust in the information furnished to the DoD and national-level decision makers. The infrastructure-wide DITSCAP standardization [4] was introduced to ensure that the shared interests of the common infrastructure are approximately represented and accounted for in the decision-making process of all the systems in the DII. Although the DITSCAP provides an excellent platform to assess the security of systems from organizational, business, technical and human perspectives, we contend that its current approach has certain limitations and drawbacks. DITSCAP is a long and exhaustive process of self-checks and documentation, requiring extensive resources to conduct, manage, and maintain, resulting in delays and huge monetary costs. Furthermore, the complex interdependencies that exist between information from large and diverse sources required to be referred and comprehended for a system to be compliant with DITSCAP, is a significant factor restricting human ability to effectively engineer secure systems that comply with DITSCAP. We identify that the lack of an organized framework and related tool support to gather and analyze the C&A related information is at the root of this problem. To deal with such issues that encompass several research areas, we propose an integrated, well-defined and comprehensive framework which combines novel techniques from requirements engineering and knowledge engineering. Such

a framework will support capturing, modeling and analyzing DITSCAP-oriented requirements, related domain knowledge, user criteria and their interdependencies across several dimensions and levels of abstractions, to identify the "*emergent features*" of the software system working as a whole, under a certain configuration in the given complex environment. In this paper, we specifically focus on automating the DITSCAP in ways that promote effective and comprehensive assessment of the operational risks and evaluation of compliance with security requirements and best practices applicable to the target system. Through the examples derived from our case study, we further motivate the appropriateness of our framework in achieving these objectives.

In the following section we provide a brief overview of the DITSCAP followed by the motivation and objectives for DITSCAP automation in section 3. In section 4, we introduce the conceptual architecture of our DITSCAP Automation Tool (DITSCAP-AT) and discuss its components. Section 5 outlines various models used in our framework that help to aggregate and analyze DITSCAP related information and demonstrates their applicability and appropriateness through examples. Finally we present our concluding remarks and future work in section 6.

2. DITSCAP OVERVIEW

DITSCAP is the standard DoD process for identifying information security requirements, providing security solutions, and managing information systems security activities [4]. DITSCAP focuses on the system mission, environment, architecture, and life cycle while assessing impact of operation of the information system on the overall security posture of the DII. The DITSCAP defines *Certification* in the context of information systems as *"Comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements"* [4]. Following the certification activities, the accreditation statement is an approval to operate the information system in a particular security mode using a prescribed set of safeguards at an acceptable level of risk by a Designated Approving Authority (DAA). It should be noted that, the relationship of the C&A process with information systems is not something that is established once to get over with, but it should be a life time commitment [6]. DITSCAP tries to fulfill this commitment by distributing its activities over four phases that range from the initiation of the C&A activities to its maintenance and reaccreditations. The level of rigor adopted for the C&A process depends on the certification level chosen for the system among the four levels available which are 1) Minimal Security Checklist; 2) Minimum Analysis; 3) Detailed Analysis; and 4) Extensive Analysis [2]. The Program Manager, DAA, Certifier and User Representative are the key roles of DITSCAP that tailor and scope the C&A efforts to the particular mission, environment, system architecture, threats, funding and schedule of the system through negotiations. Once the system definition has been agreed upon by the key roles of DITSCAP, it is documented and becomes the Software Security Authorization Agreement (SSAA). The SSAA is used throughout the DITSCAP process to guide actions, document decisions, specify IA requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security [4].

3. DITSCAP-AT MOTIVATION AND OBJECTIVES

The DITSCAP Application Manual [2] outlines a list of tasks and activities to be carried out along with the roles and responsibilities of the associated personnel. Although DITSCAP is well-defined, it is expressed at a very abstract level to maintain general applicability. This inherent abstractness coupled with a manual approach makes it hard to ensure objectivity, predictability and repeatability in practicing the DITSCAP in real world settings. Furthermore, the DITSCAP requires a multitude of DoD directives and security requisites, for a system to be compliant with, that address a diversity of factors across several dimensions at various levels of abstractions to determine the applicable security requirements. We also identify that a structured and comprehensive method to assess and monitor the operational risk of information systems is also missing in the current approach. To further aggravate the situation, the DITSCAP often becomes a mere bureaucratic necessity to get approval to operate by generating an SSAA, without specific focus on assessing and managing the operational risks of the site and system, which is the key to its effectiveness. We believe that DITSCAP-AT will reduce certification costs, resulting from the need of fewer resources to conduct, manage and maintain the C&A process, by providing an integrated environment to articulate the C&A efforts. Also, such an integrated environment is inevitable to maintain efficiency of C&A activities to significantly reduce the development and deployment time of information systems. All these factors advocate a strong and urgent need for a well-defined and comprehensive framework for DITSCAP automation, to gain the high level of trustworthiness required from the services of the information systems in the DII.

Since the problems mentioned above apply to several research areas, an integrated solution for DITSCAP automation must be engineered synergistically to incorporate the followings. Firstly, a methodology to establish the extent to which an information system meets the DITSCAP-oriented security requirements, which supports the process of identifying, interpreting and evaluating the applicable requirements based on user criteria, at various levels of abstractions. This includes tool assistance throughout DITSCAP by a well-organized flow of tasks in different activities of secure systems engineering process to populate system models that are easy to understand and analyze. Secondly, a structured, justifiable and repeatable methodology to collect threat, vulnerability and mission criticality information from a broad spectrum of sources, technical and non-technical for evaluating cost versus risk trade-offs. And finally, tool support for actively discovering and monitoring network related vulnerabilities to compare the intended and the actual operational environments. Currently we limit the scope of DITSCAP-AT to level one DITSCAP certification as applied to LAN systems only.

4. DITSCAP-AT CONCEPTUAL ARCHITECTURE

The DITSCAP-AT conceptual architecture is shown in Figure 1. We now discuss each one of its three modules in further detail.

4.1 Process-driven Workflow

The Process-driven Workflow module aims to guide the key roles of the DITSCAP through the C&A process, to elicit and capture information required for satisfying the goals of the DITSCAP.

The tasks outlined in the DITSCAP application manual [2] are extracted and homogeneously grouped into process components (P_1, P_2…P_n) as shown in Figure 1, based on their interdependent goals/objectives. Such C&A goals contained in each process component are expressed using carefully designed questionnaires/forms embedded into wizard-based interfaces designed to fill out necessary parts of the SSAA, and create and gather well-defined metrics and measures that are amenable to automated analysis. The process components also retrieve applicable requirements/policies/meta-knowledge from the Requirements Repository as well as network discovery and monitoring information from the Multi-strategy Machine Discovery module to assist the C&A process.

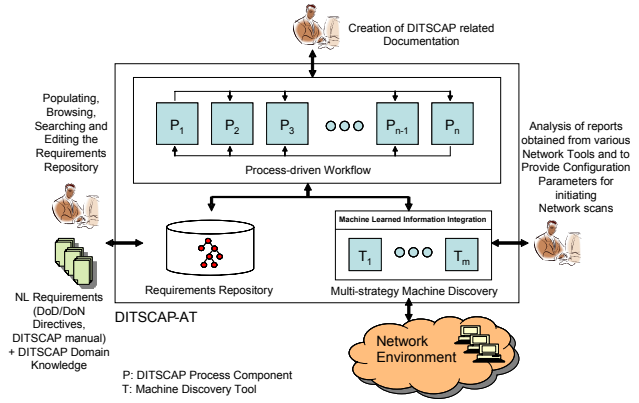

Figure 1: DITSCAP-AT Conceptual Architecture

In order to actively support the C&A process, uniformly across the DII, we create a DITSCAP Problem Domain Ontology (PDO) that provides the definition of a common language and understanding at various levels of abstractions from several dimensions through the application domain concepts, properties and their relationships in the universe of discourse i.e. the DITSCAP domain. The DITSCAP PDO is a machine understandable, structured representation of the DITSCAP, enforced security requirements and DITSCAP related domain knowledge which is stored using an object-oriented ontological representation in the Requirements Repository (Section 4.2). In the context of the Process-driven Workflow module, the DITSCAP PDO guides the C&A process through an organized flow of defined tasks and activities as well as identifies the cascading effects of changes in C&A related data via its traceable rationales.

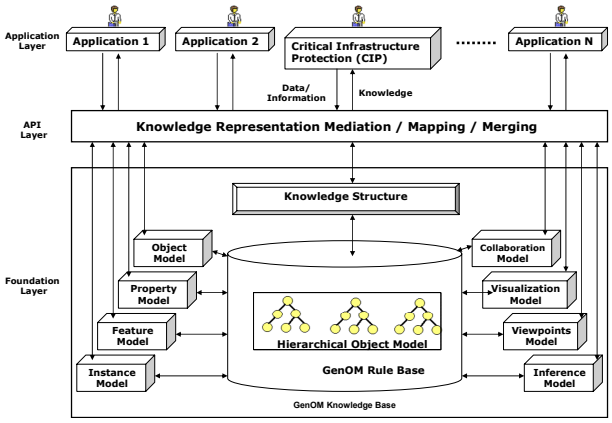

Figure 2: GenOM Conceptual Architecture

4.2 Requirements Repository

The Requirements Repository module leverages several advanced knowledge engineering techniques to support representation of requirements, meta-knowledge creation, and ability to query and browse pre-classified and categorized information structures with inference functionalities. It is a specialized module built upon the GENeric Object Model (GenOM) [10], an integrated development environment for ontological engineering processes with functionalities to create, browse, access, query and visualize associated knowledge-bases. A self explanatory conceptual architecture of GenOM is shown in Figure 2.

4.3 Multi-Strategy Machine Discovery

The Multi-Strategy Machine Discovery module supports network self-discovery capabilities that allow comparison of the intended and operational environments. It consists of a set of network tools selected on the basis of the information required for DITSCAP, such as 1) hardware, software and firmware inventories; 2) configuration information of network devices and services; and 3) vulnerability assessment using penetration testing. The multi-strategy machine discovery technique employs a combination of network discovery tools and scripts to gather and fuse aggregated information as meta-knowledge in the requirements repository, which is then suitably transformed for inclusion in the SSAA.

In the next section we discuss some of the key models in the DITSCAP automation framework used to aggregate and analyze information related to the C&A process to satisfy DITSCAP goals and objectives.

5. THE DITSCAP AUTOMATION FRAMEWORK

Traditionally, software developers have restricted their focus only to the software system attributes, but the software system itself is embedded within an environment that caters to the real world goals of the associated business and organization. This concept is even more relevant for secure system engineering processes as security is not something that can be operationalized as a single module but rather it is the "*emergent feature*" of the software system, working as a whole, under a certain configuration in the given complex environment. Therefore, an integrated and comprehensive framework that adopts a system's perspective, encompassing organizational, business, process, technical and human perspectives for enabling secure systems engineering practices is inevitable to successfully exercise the DITSCAP. To cope with such necessities, the DITSCAP PDO is aimed to provide the necessary means to understand and evaluate the effects of system functions and constraints in light of the concepts, properties their relationships that exist in the application domain from the perspectives of the real world goals, technology, organization, and business/mission requirements.

The DITSCAP PDO specifically includes structured and well-defined representations of: 1) A requirements domain model based on DITSCAP-oriented directives, security requisites and policies; 2) A risk assessment taxonomy that includes links between related risk sources and leaf node questionnaires with predictable answers that have risk weights and priorities assigned to them; 3) Overall DITSCAP process aspect knowledge that includes C&A goals/objectives; 4) Meta-knowledge about information learned from network discovery/monitoring tools; and 5) Interdependencies between entities in the DITSCAP PDO.

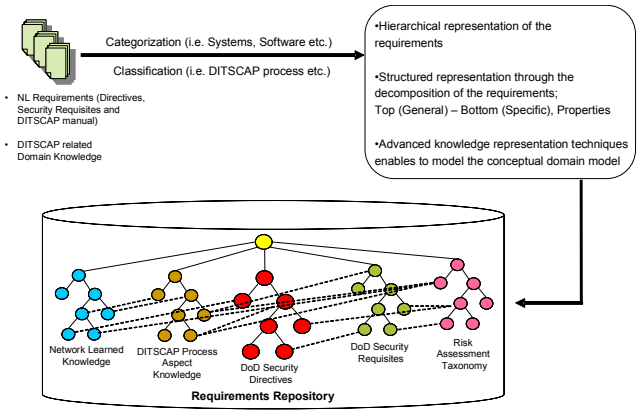

Figure 3: Populating the Requirements Repository

The methods and features of deriving such a PDO for DITSCAP are described in Figure 3. It specifically involves categorization and classification of natural language requirements expressed in DoD directives/security requisites and DITSCAP related domain knowledge. The resulting hierarchical representation includes high-level generic requirements, mid-level domain spanning requirements and sub-domain requirements in the leaf nodes. Furthermore, advanced knowledge representation techniques supported by GenOM, enable modeling of DITSCAP related domain knowledge as well. Finally, all domain models obtained through this process reside in the requirements repository. We now discuss some important representations of the models in the DITSCAP PDO in further detail.

5.1 DITSCAP C&A GOAL HIERARCHY

The goals of the DITSCAP are systematically extracted from the well-defined tasks and activities in [2] to create a hierarchical representation of the overall DITSCAP process aspect knowledge using methods identified in Figure 3.

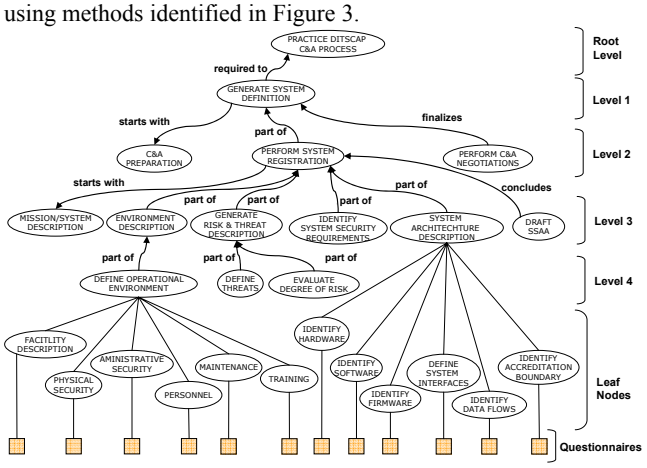

Figure 4: Partial DITSCAP C&A Process Goal Hierarchy

The user/system criteria required to evaluate the satisfaction of C&A goals in the leaf nodes of the goal hierarchy are elicited using carefully designed questionnaires presented to DITSCAP-AT users using wizard-based interfaces. A part of such a goal hierarchy is shown in Figure 4. Furthermore, a space of applicable requirements is created through the mappings between the goals in the goal hierarchy and the requirements in the Requirements Domain Model (RDM) (see subsection 5.2) at the level of corresponding abstractions.

5.2 REQUIREMENTS DOMAIN MODEL

From the analysis of DITSCAP-oriented security directives, instructions, requisites and policies, we identify that they are organized in a hierarchical fashion as shown in Figure 5.

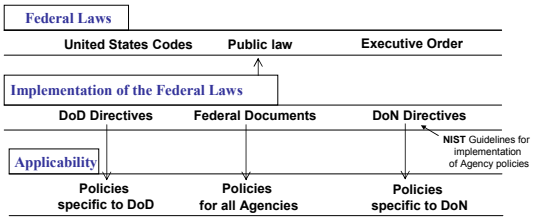

Figure 5: Organization of DITSCAP-oriented Documents

Using this inherent organization of documents and the methods and features identified in Figure 3, we create a hierarchical organization of security requirements, carefully extracted and annotated with several attributes to form a RDM. Such a hierarchical representation includes high-level Federal laws, mid-level DoD/DoN policies, and site-specific requisites in the leaf nodes. Also, there exists several non-taxonomic links that represent relationships within the RDM as well as with other entities in the PDO. A partial RDM related to requirements for a 'security plan for information systems' is shown in Figure 6, which elaborates on *Physical and Environmental Security Controls* and *Personnel Controls* as an example. Such a RDM allows the use of a goal-driven elicitation strategy to determine the applicable security requirements by successively decomposing the high-level security goals to be achieved by the system into a set of specific applicable requirements from DITSCAP enforced directives and security requisites. Furthermore, the non-taxonomic interdependencies between different requirements can be utilized to identify related requirements from other categories that may be overlooked. The RDM, along with other models in the DITSCAP PDO, can effectively establish the extent to which an information system meets the DITSCAP specified security requirements by supporting the process of identifying and interpreting the applicable requirements based on user criteria. This becomes more evident through examples discussed in subsection 5.5.

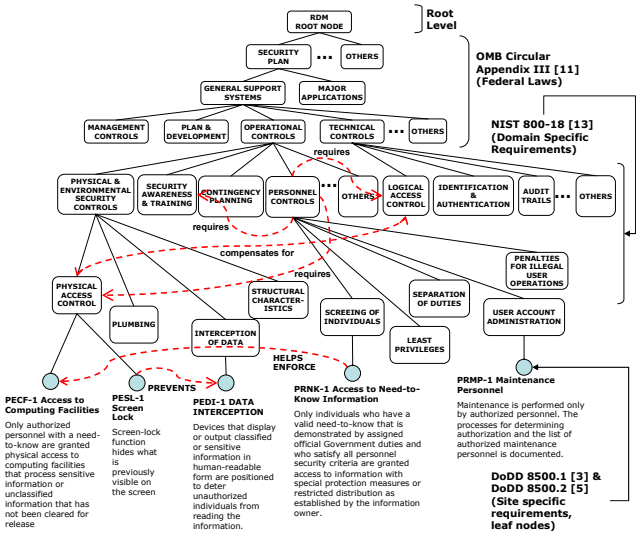

Figure 6: A Partial RDM for a Security Plan

5.3 RISK ASSESSMENT TAXONOMY

Based on the DITSCAP goals for risk assessment, we identify the need for a methodology that aggregates risk information from the site and system, and relates it to the overall security posture. Also, such a methodology should be anchored in objective metrics and measures that can be evaluated and interpreted in a uniform way across the infrastructure.

To satisfy these criteria we create a Risk Assessment Taxonomy in the DITSCAP PDO which aggregates a broad spectrum of possible categories and classification of risk related information in the DITSCAP domain. The risk assessment goals expressed in the higher level non-leaf nodes of this taxonomy can be achieved using specific criteria addressed in the leaf nodes. An example risk assessment taxonomy is shown in Figure 7. Such a taxonomy provides a structured and comprehensive view of various risk categories associated with the site and system from a variety of different perspectives. The risk taxonomy in the upper level non-leaf nodes consists of threat, vulnerabilities, countermeasures, mission criticality, asset value and other categories related to risk assessment. Each non-leaf node is then further decomposed into more specific categories. In our work, the scope of the risk related categorization is mainly based on the National Information Assurance Glossary [1] as well as other sources such as the DITSCAP Application Manual [2], DITSCAP Minimal Security Checklists [2] and network related vulnerabilities discovered using the multi-strategy machine discovery module.

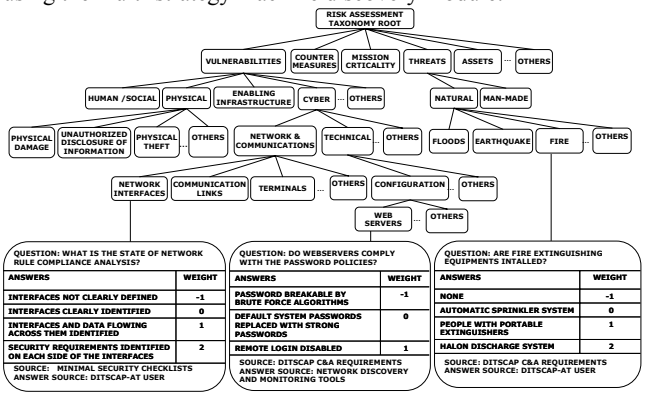

Figure 7: Example Risk Assessment Taxonomy

A predictable and quantitative risk assessment can be carried out using weights assigned to pre-classified answers for specific questionnaires/criteria in the leaf nodes. These answers can be elicited from a variety of sources such as DITSCAP-AT users, using network self-learned information, or other sources. Example leaf node questions under various categories are also shown in Figure 7. Higher weights are assigned to answers related to lower risk levels following risk reduction scoring techniques. Other auxiliary information such as source of question and answer can be used to associate additional priority/criticality and traceability for each leaf node. Also, it is worthy to note that the questionnaires/criteria in the leaf nodes usually relate to various security requirements in the RDM by expressing their testability in the form of criteria through which level of requirements compliance can be measured. As the risk assessment taxonomy gets populated with answers to questionnaires/criteria in the leaf nodes, a comprehensive collection of risk related information is available which can be used to perform complex risk calculations and form the basis for evaluating cost versus risk trade-offs.

5.4 VIEWPOINTS HIERARCHY

Requirements usually capture ideas, perspectives and relationships at various levels of detail and they are interpreted differently from different viewpoints. Considering this and following the concepts put forth in [12], [9] and [7] we use the viewpoints hierarchy as a natural way to organize and structure the diversity of factors associated with requirements in the DITSCAP PDO. The higher level non-leaf nodes in the viewpoints hierarchy specifically consists of viewpoints, such as organizational viewpoints (In DITSCAP domain, an example would be *The DoD Components* that refers to all organization entities in the DoD [4]), which map to generic requirements in the RDM, and the lower level leaf nodes representing viewpoints such as those of system stakeholders or services that are related to site-specific requirements in the leaf nodes of the RDM. For each DITSCAP-oriented security requirement, viewpoints are extracted from the related documents by identifying associated stakeholders. For identifying/organizing viewpoints we adopt the abstract viewpoints classes as defined by the VORD [7] approach. In the next subsection we introduce, using examples, the concept of multi-dimensional link analysis.

5.5 MULTI-DIMENSIONAL LINK ANALYSIS (MDLA)

The root of MDLA lies in the concept of the viewpoints model introduced in the PVRD methodology proposed by Lee [9]. Lee suggests that "*Individual pieces of information finally become valuable knowledge when they establish 'links' with each other from various aspects/dimensions based on a certain set of goals*". Following this paradigm, MDLA can be carried out from various aspects such as, business/mission requirements, regulatory requirements, user criteria, specific operational concepts, viewpoints and risk categories based on the DITSCAP C&A goals. The DITSCAP PDO that resides in the requirements repository using a uniform representation scheme fosters such analysis due to its inherent properties and characteristics.

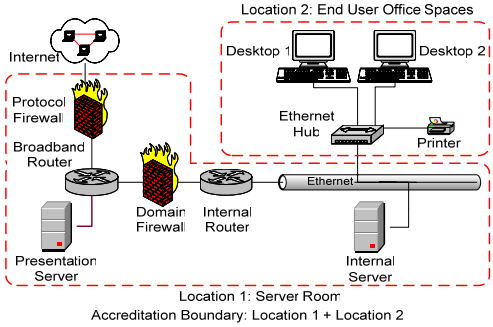

Figure 8: Hypothetical Networked Information System

The user criteria and system configuration captured using well designed questionnaires and network self-discovery capabilities of DITSCAP-AT act as trigger mechanisms for MDLA. The goals in the C&A goal hierarchy project a certain search/applicability space of requirements in the RDM that includes potentially applicable requirements to the related user criteria. More abstract the goal, larger the search/applicability space of requirements is in the RDM. Once the search space has been identified from the goals, the related user criteria can be analyzed further to identify the applicable security requirements and their interdependencies with other entities in the DITSCAP PDO. Furthermore, for each

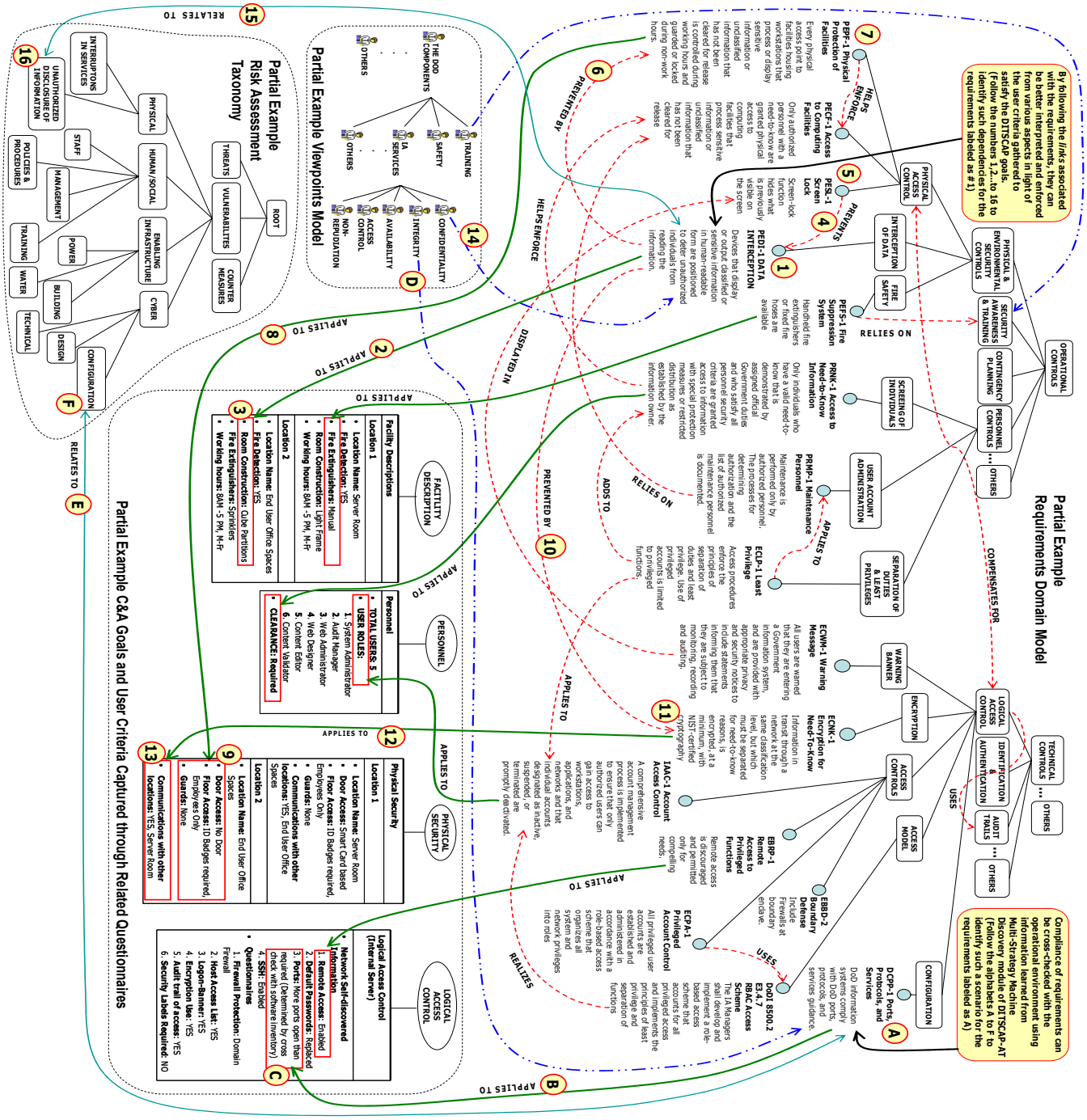

Figure 9: Multi-dimensional Link Analysis

requirement in the RDM, the viewpoints associated with it, as well as the related risk information in the risk assessment taxonomy contribute to the ways in which the "*emergent behavior*" of the system can be comprehended.

The example information system, as shown in Figure 8, is a web hosting site that makes available DoD policies and procedures on the internet for public access. We consider the following C&A goals and the associated user criteria for analysis: 1) Identify *Personnel Controls;* 2) Gather *Facility Descriptions;* 3) Identify *Physical Access Controls;* and 4) Identify *Logical Access Controls*. Snippets of information collected by DITSCAP-AT about the user criteria and system configuration, to satisfy each of these goals, is shown in Figure 9. It should be noted that the information is gathered from DITSCAP-AT users in a way that avoids misguidance to attain C&A. Figure 9 shows a simplified example of the mapping of specific user criteria to the applicable requirements in the RDM and the relationships of these requirements with other models in the DITSCAP PDO, modeled using ontology modeling constructs. By following the *links* associated with each requirement, they can be better interpreted and enforced from various aspects in light of the user criteria gathered to satisfy the DITSCAP goals. For example, the

requirement *PEDI-1 Data Interception* (marked as "1" in the RDM of Figure 9), *Applies To* the user criteria for C&A goal of *Facility Description* for *Location 2*, of the network in Figure 8, which states that the *Room Construction* type is *Cube partitions*. This requirement is applicable as the user criterion contributes to display of sensitive information on monitors of end user desktops placed in open cubicles. Such *links* helps to understand "what & why" a particular requirement is applicable to a system in a particular setting. To effectively assess and enforce this requirement in combination with several technical and non-technical factors in the environment, we observe the relationship of this requirement with other requirements in the RDM as well as entities in other models of the DITSCAP PDO. Within the RDM, the *PEDI-1 Data Interception* requirement has relationships with requirements under the *Physical Access Control* category as well as *Logical Access Control* category. Under the *Physical Access Control* category, it can be identified from the relationships that both the requirements *PESL-1 Screen Lock* and *PEPF-1 Physical Protection of Facilities* help to *Prevent* data interception. Furthermore, the *PEPF-1 Physical Protection of Facilities* requirement *Applies To* the C&A goal of *Physical Security* for *Location 2*, whose user criteria indicates absence of guards and doors, which is in violation for that requirement. This violation in turn contributes to the risk associated with *PEDI-1 Data Interception* in these settings. Under the *Logical Access Control* category, the *ECNK-1 Encryption for Need-To-Know* requirement *Prevents* data interception using the encryption of data in transit through network to other locations. The *ECNK-1 Encryption for Need-To-Know* requirement further *Applies To* the user criteria, for C&A goal of *Physical Security* for *Location 2,* of *Communication with other locations*, indicating the need for encrypting the transmission of data between *Location 1* and *Location 2* to prevent data interception. The *PEDI-1 Data Interception* requirement is also related to the viewpoint of *Confidentiality*, which helps to understand the specific IA objectives satisfied by enforcing the requirements in terms of the IA services provided by the system. Furthermore, the risks associated with the *PEDI-1 Data Interception* requirement can be aggregated under the related risk category of *Unauthorized Disclosure of Information* in the risk assessment taxonomy, which in turn contributes to the overall risk calculation for the system.

Similarly, several requirements for the C&A goals of identifying *Personnel Controls* and *Logical Access Controls* (follow labels "A" to "F" in Figure 9) can be brought into focus and analyzed using MDLA method as shown in Figure 9. Such analysis can also reveal the missing requirements [9], that weren't apparent at the onset of the C&A process by providing a comprehensive analysis of the information system under consideration.

Through the theoretical foundations of the DITSCAP automation framework, complex interdependencies between the information systems and their environments can be systematically captured, modeled, analyzed and comprehended to realize secure systems engineering practices for critical infrastructure components.

6. CONCLUSION AND FUTURE WORK

In this paper, we specifically focus on automating the C&A processes, as prescribed by the DITSCAP. We identify that the contribution of DITSCAP-AT is two fold. Firstly, it provides a structured and comprehensive framework to aggregate and analyze C&A related information at various levels of abstractions, using a uniform representation scheme, allowing for its reuse and evolution through all stages of a secure software engineering lifecycle. Secondly, it provides these functionalities through appropriate tool support for the C&A process that facilitates its adoption and practice throughout the infrastructure. Although the scope and limited space of this paper does not allow us to discuss all aspects of our framework in detail, we have engineered our framework as an integrated and unique combination of techniques that facilitates eliciting and capturing of requirements and specifications, modeling of system environments and domain knowledge, managing software evolution and adaptability to change and, supporting analysis and design processes through decision support and traceability. Such a framework is inevitable for advanced software/system engineering practices to produce secure systems with a high level of trust in their services.

Our on-going and future work includes the software realization of DITSCAP-AT conceptual design based on the requirements elicited using mock-up interfaces that provide a thorough understanding of the important aspects of its user interaction [8]. Furthermore, with the availability of an integrated environment for DITSCAP automation, the development of formalized metrics and measures for a comprehensive and uniform risk assessment in the DITSCAP domain is an area that requires significant attention in our future work for the success of this initiative.

ACKNOWLEDGMENTS

This work is partially supported by the grant (Contract: N65236-05-P-0597) from the Critical Infrastructure Protection Center, Space and Naval Warfare Systems Center, Charleston, SC. USA. The authors acknowledge the support from Scott West, John Linden, Bill Bolick, and Bill Chu. Finally, the authors thank Deepak Yavagal and Divya Muthurajan for their contributions.

7. REFERENCES

[1] CNSS 4009. *National Information Assurance Glossary*. NSA, 2003.

[2] DoD 8510.1-M. *DITSCAP Application Manual*. July 2000.

[3] DoD 8500.1. *Information Assurance*. Oct. 2002.

[4] DoD 5200.40. *DITSCAP*. December 1997.

[5] DoD 8500.2. *Information Assurance Implementation*. Feb. 2003.

[6] Kimbell, J. and Walrath, M. Life Cycle Security and DITSCAP. *IANewsletter*, Vol. 4(2), Spring 2001.

[7] Kotonya, G. and Sommerville, I. Requirements Engineering with Viewpoints. *BCS/IEE Software Engineering Journal*, pp. 5-18, Vol. 11, Issue: 1, Jan. 1996.

[8] Lee, S.W., Ahn, G. and Gandhi, R.A. Engineering Information Assurance for Critical Infrastructures: The DITSCAP Automation Study. In *Proceedings of the Fifteenth Annual International Symposium of the International Council on Systems Engineering (INCOSE '05)*, Rochester, NY, July 10-15. 2005.

[9] Lee, S.W. and Rine, D.C. Missing Requirements and Relationship Discovery through Proxy Viewpoints Model. *Studia Informatica Universalis: Int'l. Journal on Informatics*, Spring 2005.

[10] Lee, S.W. and Yavagal, D. *GenOM User's Guide*. Technical Report TR-SIS-NISE-04-01, Dept. of Software and Information Systems, UNC Charlotte, Spring 2004.

[11] Office of Management and Budget (OMB) Circular No. A-130: Management of Federal Information Resources, 1996.

[12] Sommerville, I. and Sawyer, P. Viewpoints: Principles, Problems and a Practical Approach to Requirements Engineering. *Annals of Software Engineering*, Vol. 3, pp. 101-130, 1997.

[13] Swanson, M. Guide for Developing Security Plans for Information Technology Systems. *NIST Special Publication 800-18*, 1998.