In Proceedings of the IEEE International Conference on Intelligence and Security Informatics (IEEE ISI-2005),
Atlanta, Georgia, May 19-20, 2005.
A Book Chapter in Lecture Notes in Computer Science, Volume 3495, pp. 479-485, Springer.

Active Automation of the DITSCAP

Seok Won Lee, Robin A. Gandhi, Gail-Joon Ahn, and Deepak S. Yavagal

Department of Software and Information Systems
The University of North Carolina at Charlotte, Charlotte, NC 28223
{seoklee, rgandhi, gahn, dsyavaga}@uncc.edu

Abstract. The Defense Information Infrastructure (DII) connects Department of Defense (DoD) mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and provides information processing and value-added services. For such a critical infrastructure to effectively mitigate risk, optimize its security posture and evaluate its information assurance practices, we identify the need for a structured and comprehensive certification and accreditation (C&A) framework with appropriate tool support. In this paper, we present an active approach to provide effective tool support that automates the DoD Information Technology Security C&A Process (DITSCAP) for information networks in the DII.

1 Introduction

The DoD increasingly relies on software information systems, irrespective of their level of classification, in order to perform a variety of functions to accomplish their missions. The DITSCAP provides an excellent platform to assess the security of software information systems from organizational, business, technical and personnel aspects while supporting an infrastructure-centric approach. However, the lack of an integrated C&A framework and tool support often diminishes its effectiveness. DITSCAP itself can be quite overwhelming due to its long and exhaustive process of cross-checks and analysis which requires sifting through a multitude of DITSCAP polices and requirements. The complex interdependencies that exist between information from such large and diverse sources, significantly restricts human ability to effectively comprehend, develop, configure, manage and protect these systems.

To address these shortcomings and enhance the effectiveness of DITSCAP, we discuss our design principles, modeling techniques and supporting theoretical foundations that lead to the conceptual design of the DITSCAP Automation Tool (DITSCAP-AT). DITSCAP-AT aggregates C&A related information from various sources using a uniform representation scheme, and transforms static record keeping repositories into active ones that link to each other from different perspectives, allowing for their reuse and evolution through all stages of the system C&A lifecycle. DITSCAP-AT combines novel techniques from software requirements engineering and knowledge engineering to leverage the power of ontologies [10] for representing, modeling and analyzing DITSCAP-oriented requirements, while actively assisting the discovery of missing, conflicting and interdependent pieces of information that are critical to assess DITSCAP compliance.

In Proceedings of the IEEE International Conference on Intelligence and Security Informatics (IEEE ISI-2005),
Atlanta, Georgia, May 19-20, 2005.
A Book Chapter in Lecture Notes in Computer Science, Volume 3495, pp. 479-485, Springer.

2 DITSCAP Overview and Objectives for its Automation

DITSCAP is a standard DoD process for identifying information security requirements, providing security solutions, and managing information systems security activities [3] for systems in the DII. DITSCAP certification is a "*comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements"* [3]. Ensuing certification, 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. DITSCAP distributes its activities over four phases that range from the initiation of the C&A activities to its maintenance and reaccreditations. The level of rigor in each phase depends on the certification level chosen for the information system among the four levels available [2]. The security plan for DITSCAP is documented in the Software Security Authorization Agreement (SSAA) to "*guide actions, document decisions, specify IA requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security*" [3].

Although the DITSCAP application manual [2] outlines the C&A tasks and activities along with associated roles and responsibilities of C&A personnel, they are expressed at an abstract level to maintain general applicability. Such abstractness makes it hard to ensure objectivity, predictability and repeatability in interpreting and enforcing DITSCAP requirements and policies. Furthermore, an entirely manual approach to cross-reference a multitude of DITSCAP-oriented directives, security requisites and policies in the light of user/system criteria to determine applicable security requirements raises serious concerns about the accuracy and comprehensiveness of such assessments. A structured and comprehensive method to assess and monitor the operational risk of information systems is also missing in the current approach.

To address the above shortcomings, the first and foremost objective of DITSCAP automation is to effectively assess the extent to which an information system meets the DITSCAP-oriented security requirements by supporting the process of identifying, interpreting and enforcing the applicable requirements based on user/system criteria. To reduce the amount of long and exhaustive documentation, carefully designed interfaces need to be developed that guide the user interactions through the DITSCAP tasks and activities. These interfaces should leverage thoroughly designed questionnaires and criteria, extracted from DITSCAP related C&A goals, directives, security requisites and other widely accepted best practices. These questionnaires along with predefined answers become the basis for building well defined metrics and measures that encompass the scope of the C&A goals addressed by them. The DITSCAP automation also demands structured, justifiable and repeatable methods to have for a comprehensive risk assessment, providing a firm basis to create cost versus risk measures. To actively discover and monitor network vulnerabilities, DITSCAP automation requires network self-discovery capabilities that allow comparison between the intended and the actual operational environment. Currently we limit the scope of DITSCAP-AT to level one DITSCAP certification as applied to Local Area Network (LAN) systems only. In the following section, we present the DITSCAP-AT conceptual architecture conceived through our analysis to accomplish the aforementioned objectives.

In Proceedings of the IEEE International Conference on Intelligence and Security Informatics (IEEE ISI-2005),
Atlanta, Georgia, May 19-20, 2005.
A Book Chapter in Lecture Notes in Computer Science, Volume 3495, pp. 479-485, Springer.

3. DITSCAP-AT Conceptual Architecture

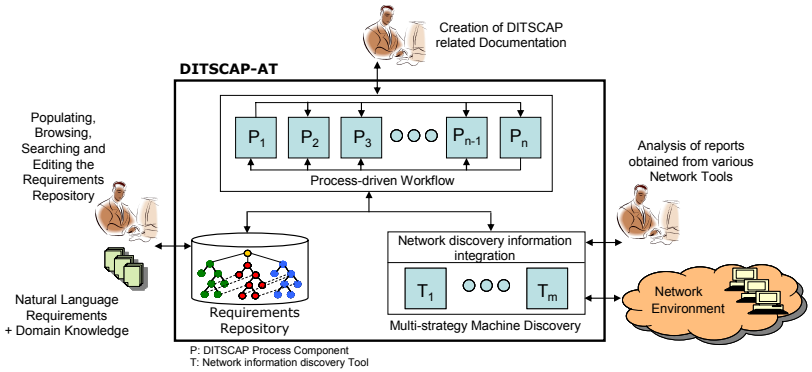

Fig. 1. DITSCAP-AT Conceptual Architecture

The conceptual architecture of DITSCAP-AT is shown in Fig. 1. The Process-driven Workflow module guides the DITSCAP through a well-defined course of action that results in the elicitation of required user criteria and generation of the SSAA. The tasks contained in each process component (P_1, $P_2 \ldots P_n$) are extracted from the DITSCAP application manual [2] and homogenously grouped based on their interdependent goals/objectives. Each task is then further expressed using carefully designed questionnaires/forms embedded in wizard-based interfaces to gather and establish well-defined C&A metrics and measures.

The Requirements Repository module provides a complete ontological engineering support for DITSCAP-AT. It provides utilities to support representation of security requirements, meta-knowledge creation, ability to query pre-classified and categorized information structures and other browsing and inference functionalities. The requirements repository is a specialized module built upon the GENeric Object Model (GenOM) [6], an integrated development environment for ontological engineering processes with functionalities to create, browse, access, query and visualize associated knowledge-bases (Ontology + Rules).

The Multi-strategy Machine Discovery module supports network self-discovery capabilities that allow the comparison of intended and operational environments. A set of network tools are selected on the basis of the information required to assess DITSCAP compliance, such as hardware, software and firmware inventories, configurations of network devices and services, and vulnerability assessment using penetration testing. A combination of network discovery tools and scripts enables to gather and fuse aggregated information as meta-knowledge in the requirements repository, which is then suitably transformed for inclusion in the SSAA.

The process components of the Process-driven Workflow module retrieve applicable requirements/policies/meta-knowledge from the Requirements Repository and network discovery/monitoring information from the Multi-strategy Machine Discovery module, to actively assist the user in the C&A process.

In the following section, we discuss the use of information aggregated by DITSCAP-AT to achieve the objectives of DITSCAP automation.

In Proceedings of the IEEE International Conference on Intelligence and Security Informatics (IEEE ISI-2005),
Atlanta, Georgia, May 19-20, 2005.
A Book Chapter in Lecture Notes in Computer Science, Volume 3495, pp. 479-485, Springer.

4 The DITSCAP Automation Framework

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 of the DITSCAP domain at various levels of abstractions through the application domain concepts, properties and relationships between them. The PDO is a machine understandable, structured representation of the DITSCAP domain captured using an object oriented ontological representation in the Requirements Repository. We elaborate more on methods and features for deriving the PDO in [7]. To satisfy the objectives of DITSCAP automation, the PDO specifically includes structured and well defined representations of: 1) A requirements hierarchy 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 PDO.

One of the objectives of DITSCAP-AT is to assess the extent to which an information system meets the DITSCAP-oriented security requirements by supporting the process of identifying, interpreting and enforcing the applicable requirements based on user criteria. The PDO supports such features through a requirements hierarchy that is constructed by extracting requirements from DITSCAP-oriented security directives, instructions, requisites and policies. A hierarchical representation includes high-level Federal laws, mid-level DoD/DoN policies, and site-specific requisites in the leaf nodes, which naturally corresponds to generic requirements, domain spanning requirements and sub-domain requirements in the requirements hierarchy. Also, there exists several non-taxonomic links that represent relationships within the requirements hierarchy as well as with other entities in the PDO.

A requirements hierarchy, therefore, allows the determination of applicable security requirements by successively decomposing the high-level generic requirements into a set of specific applicable requirements in the leaf nodes based on user criteria. Furthermore, the non-taxonomic links can be utilized to effectively interpret and enforce requirements by identifying the related requirements in other categories as well as relationships with entities in various dimensions from the PDO to ensure a comprehensive coverage of the C&A process.

To address the needs for a structured, justifiable and repeatable method for a comprehensive risk assessment, the PDO includes a risk assessment taxonomy which aggregates a broad spectrum of all possible categories and classification of risk related information. 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. For example, 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 addition, several non-taxonomic links identify relationships with other risk categories as well as with other entities in the PDO. Current 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]

In Proceedings of the IEEE International Conference on Intelligence and Security Informatics (IEEE ISI-2005),
Atlanta, Georgia, May 19-20, 2005.
A Book Chapter in Lecture Notes in Computer Science, Volume 3495, pp. 479-485, Springer.

and the DITSCAP Minimal Security Checklist [2]. We also utilize the information security metrics that have been established by the National Institute of Standards and Technology [8], [9].

A predictable and quantitative risk assessment is carried out using weights assigned to pre-classified answers for specific questions/criteria in the leaf nodes. These answers can be elicited from a variety of sources such as DITSCAP-AT users, network self-discovered information, or other sources. Furthermore, the questions/criteria in the leaf nodes of the risk assessment taxonomy naturally relate to various security requirements in the requirements hierarchy by expressing their testability in the form of criteria to measure their level of compliance. Such relationships along with the priorities/weights/criticalities associated with answers to questions/criteria in the leaf nodes of the risk assessment taxonomy can be used to develop complex risk calculation algorithms and establish metrics and measures that enable further articulation of critical weakest points in the system. The risk assessment taxonomy also promotes a uniform and comprehensive interpretation of different risk categories that are established through a common understanding of the concepts, properties and relationships that exist in the DITSCAP PDO. Such a shared understanding is inevitable to effectively estimate the collective impact of residual risk from all supporting systems on the overall critical infrastructure.

To populate the models discussed here, we have designed several core mock interfaces for DITSCAP-AT to realize a complete course of action for gathering and analyzing the required information [7]. Such mock interfaces provide a thorough understanding of the important aspects of DITSCAP-AT user interaction and offer valuable insight and assurance in realizing the theoretical aspects of DITSCAP automation.

5 Multi-dimensional Link Analysis

The root of Multi-Dimensional Link Analysis (MDLA) lies in the concept of proxy viewpoints model from the PVRD methodology proposed by Lee [5] to discover missing requirements and relationships. 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 different dimensions such as user criteria, viewpoints [4], system goals, business/mission requirements, regulatory requirements, specific operational concepts, and risk categories based on the DITSCAP C&A goals which can help understand various interdependencies between DITSCAP-oriented requirements, facilitating their interpretation and enforcement. The DITSCAP PDO that resides in the requirements repository fosters such analysis due to its ontological characteristics that provides inherent properties for an active approach to link requirements and other entities from different perspectives and dimensions. MDLA's integrated framework for analytical analysis promotes assurance for a comprehensive coverage of the certification compliance space by actively assisting the process of discovering missing, conflicting, and interdependent pieces of information as well as establishing C&A metrics and measures based on common understanding and the reflected language from various dimensions.

5 Conclusion and Future Work

DITSCAP-AT contributes to the automation of DITSCAP in several ways. Firstly, it provides an effective tool support to identify, interpret and enforce DITSCAP polices and requirements. Secondly, it provides a structured and comprehensive approach to risk assessment from a broad spectrum of categories contributing to risk and finally, the ability to perform multi-dimensional link analysis provides the opportunity to reveal the "emergent" or "missing" information pieces that in-turn provides the assurance of a comprehensive coverage of the certification compliance space.

Our future work includes the software realization of DITSCAP-AT mock interfaces while systematically realizing all its core functional components. Although we limit the current scope of DITSCAP-AT to include DoD directives, security requisites and best practices for secure software development, it can be easily scaled to accommodate general security requirements, policies and practices in any domain of interests. We also realize that development of appropriate metrics and measures for a comprehensive and uniform risk assessment in the DITSCAP domain is an area that requires significant attention for the success of DITSCAP-AT.

Acknowledgements
This work is partially supported by the grant (Contract: N65236-05-P-0597) from the Critical Infrastructure Protection Center (CIPC), Space and Naval Warfare (SPAWAR) Systems Center, Charleston, SC. USA. We acknowledge the support and encouragement from Scott West, John Linden, Bill Bolick, and Bill Chu. Finally, we thank Divya Muthurajan and Vikram Parekh for their contributions to this research.

6 References

1. Committee on National Security Systems (CNSS) Instruction No. 4009.: National Information Assurance (IA) Glossary. (2003)
2. DoD 8510.1-M: DITSCAP Application Manual (2000)
3. DoD Instruction 5200.40.: DITSCAP (1997)
4. Kotonya, G. and Sommerville, I.: Requirements Engineering with Viewpoints. BCS/IEEE Software Engineering Journal, Vol. 11, Issue 1 (1996) 5-18
5. Lee, S.W. and, Rine D.C.: Missing Requirements and Relationship Discovery through Proxy Viewpoints Model. Studia Informatica Universalis: International Journal on Informatics, December (2004)
6. Lee, S.W. and, Yavagal, D.: GenOM User's Guide. Technical Report: Dept. of Software and Information Systems, UNC Charlotte (2004)
7. Lee, S.W., Ahn, G. and Gandhi, R.A.: Engineering Information Assurance for Critical Infrastructures: The DITSCAP Automation Study. To apprear in: Proceedings of the Fifteenth Annual International Symposium of the International Council on Systems Engineering (INCOSE '05), Rochester New York July (2005)
8. Swanson, M., Nadya, B., Sabato, J., Hash, J., Graffo, L.: Security Metrics Guide for information Technology Systems. NIST #800-55 (2003)
9. Swanson, M.: Security Self-Assessment Guide for Information Technology Systems. NIST #800-26 (2001)
10. Swartout, W. and Tate, A.: Ontologies. In: Intelligent Systems, IEEE, Vol. 14(1) (1999)