To appear in Proceedings of the 13th IEEE International Requirements Engineering Conference (RE '05)
Symposium on Requirements Engineering for Information Security (SREIS 05), 8/29 – 9/2, Paris, France, IEEE Press.

Security Requirements Driven Risk Assessment for Critical Infrastructure Information Systems

Seok-Won Lee, Robin A. Gandhi and Gail-Joon Ahn
Dept. of Software and Information Systems, The University of North Carolina at Charlotte
Charlotte, NC 28223-0001, USA. *{seoklee, rgandhi, gahn}@uncc.edu*

Abstract

Major information processing and associated value-added services provided by information systems in critical infrastructures are being increasingly used for various purposes irrespective of their security posture. Although several infrastructure-wide standard security Certification and Accreditation (C&A) processes exist, their effectiveness in the real world is challenged by the complexity of information systems and their diverse socio-technical operational environments. We identify that these factors naturally demand the integration of several modeling techniques, to adequately support the breath and depth of C&A processes, with complementary semantics and levels of abstraction to elicit, represent and analyze the diversity of factors associated with the system under consideration. Furthermore, to promote cohesiveness between the artifacts captured through this approach, we identify the need for a comprehensive framework that allows them to synergistically understand and link to each other through the application domain concepts, properties and their relationships. In this paper, we specifically focus on the interactions between various models within such a framework based on the relationships between security requirements and the elements of risk assessment for driving an objective, repeatable and justifiable risk assessment process.

1. Introduction

The 2004 Federal Information Security Management Act (FISMA) Computer Security report card [19] has given an average D+ grade to the security posture of government-wide computer systems. The report depicts a grave security situation which questions the trustworthiness of computer systems used for storing, processing and maintaining the information being used by national-level decision makers. This situation calls for significant improvements in Certification and Accreditation (C&A), annual testing, and security training to maintain the Information Assurance (IA) and security posture of the information systems that are operational in such critical infrastructures. The cornerstone of IA assessment is the C&A process, which is designed to evaluate various entities (Organization, Process, Product or Practices) against certain quantifiable criteria for the procurement of certification based on established metrics and measures. Following 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.

Although there exists several infrastructure-wide standard security C&A processes in various formats [2] [3] [5] [22], the ever-growing complexity of information systems operating in inherently dynamic and multifaceted socio-technical environments pose significant challenges to their effectiveness in the real world. Typically C&A processes mandate extensive documentation and analysis but lack the means to systematically understand and predict the emergent system behavior from the gathered information. These issues naturally demand the integration of several modeling techniques that help to capture and understand the collective influence of various factors that impact the secure operation of a system. To adequately support the breath and depth of C&A processes, such an integrated approach provides complementary semantics and levels of abstraction to effectively elicit, represent and analyze the diverse factors associated with the system under consideration. Furthermore, to promote cohesiveness between the artifacts captured through this approach, we identify the need for a comprehensive framework that allows them to synergistically understand and link to each other through the application domain concepts, properties and their relationships. Effectively, the framework provides the definition of a common language that supports interaction and traceability between different system models at various levels of abstraction [10].

In this paper, we focus on the Department of Defense Information Technology Security C&A Process (DITSCAP) [5], a standard for systems operational in the Defense Information Infrastructure (DII). The DII is an interconnected network of computers, communications, data, applications, security, people, training, and other support structure, serving the Department of Defense's (DoD) local and worldwide information needs. The services made available through the DII are 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. Although the DITSCAP is an excellent platform to assess the security and risks faced by information systems from organizational, business, technical and human perspectives, it suffers from several shortcomings of the current C&A processes discussed earlier in this section. To address these limitations of the DITSCAP, based on our approach we utilize several modeling techniques within the DITSCAP automation framework [11] to assist the C&A activities. The models defined within the framework allow us to systematically utilize the mappings that exist between the security requirements enforced by DITSCAP and the elements of risk assessment to drive an objective, repeatable and justifiable risk assessment process. More specifically, the artifacts related to security requirements and the risk factors applicable to a target system synergistically link to each other through the concepts, properties and their relationships captured within the DITSCAP automation framework. We present our approach and demonstrate its applicability and appropriateness using examples derived from our case study on automating the DITSCAP.

The paper is organized as follows. In the following section we provide a brief overview of risk assessment in the DITSCAP and its challenges. Section 3 provides a summary of the DITSCAP automation framework and the underlying models which assist C&A process. In section 4, we uncover the mappings that exist between security requirements and risk factors. These relationships then help us in defining a risk assessment methodology in the DITSCAP automation framework in Section 5. We present related work and conclusions in sections 6 and 7, respectively.

2. Risk Assessment in the DITSCAP

The DITSCAP defines risk assessment as the process of analyzing threats to and vulnerabilities of an information system and the potential impact that the loss of information or capabilities of a system would have on national security [4]. The resulting analysis is used as a basis for identifying appropriate and cost-effective measures to either eliminate or reduce the capabilities of the threat agent or the corresponding vulnerability. The goal is to obtain “*adequate security*” which is defined in [17] as “*security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.*” This definition explicitly emphasizes the “*risk-based*” policy for a cost-effective security established by the Computer Security Act [18]. Following DITSCAP a threat assessment is developed during Phase 1 of the process and then vulnerabilities are identified by testing and analysis in Phase 2 and 3.

The DITSCAP Application Manual [4] advocates that risks may be identified during normal operations or as a result of a C&A effort, risk analysis, or an incident. The DITSCAP does not require the preparation of a formal risk analysis or assessment. It is argued in [4] that rather than trying to precisely measure risk, security efforts are better served by generally assessing and understanding risks and taking actions to manage them. But we identify that the major challenges encountered in comprehending such risks in the DITSCAP domain are: 1) The ever-growing complexity of information systems and highly convoluted relationships between their components; 2) Inherently dynamic and multi-faceted socio-technical operational environments; 3) The emergent nature of risk factors which become apparent only after system is operational or integrated; 4) An entirely manual and informal/adhoc approach to risk assessment; 5) Diversity of dimensions (e.g. security, safety, survivability, etc.) from which risk factors can be addressed at various levels of abstractions; and 6) A wide-range of stakeholders associated with the system which evaluate the risk associated with the system from different perspectives.

To address these challenges and effectively assist C&A tasks and activities we utilize several modeling techniques with differing semantics and levels of abstraction to elicit, represent and analyze the information necessary to assess risk. Finally, the models produced through these techniques within a unifying DITSCAP automation framework [11] form links with each other to understand and analyze the information gathered through the C&A process. We now provide a brief overview of the DITSCAP automation framework in the following section.

3. The DITSCAP Automation Framework

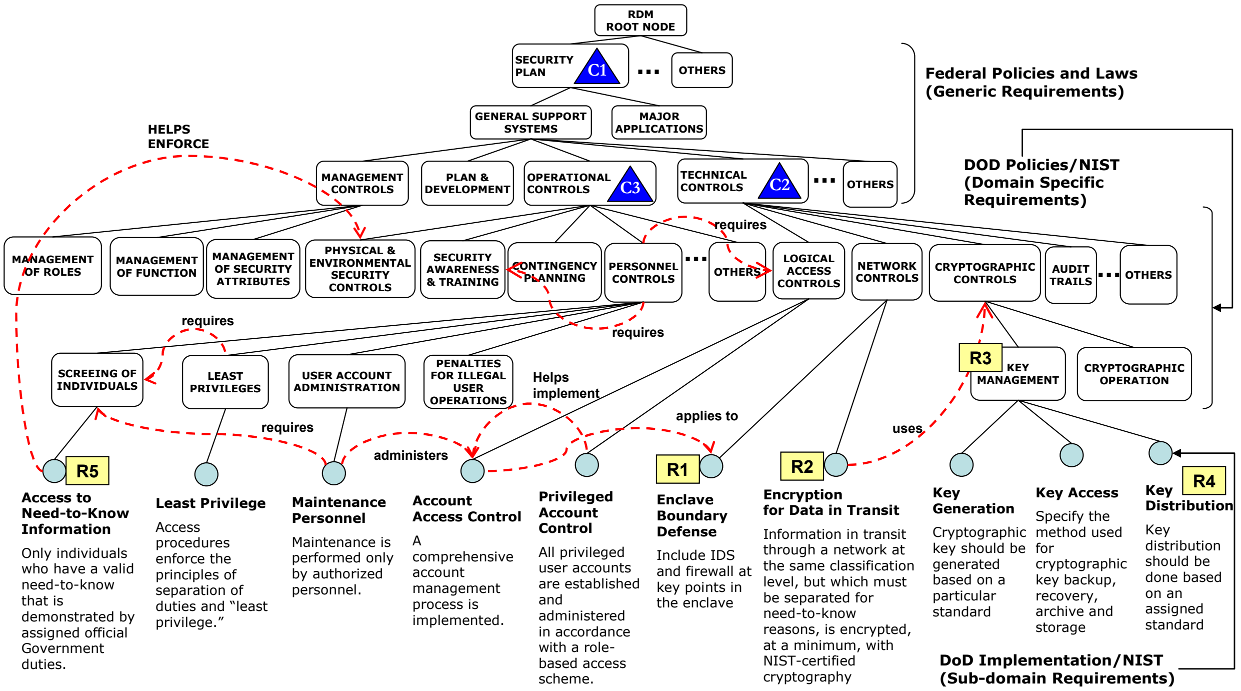
The DITSCAP itself is a long and exhaustive process of self-checks and documentation, requiring extensive resources to conduct, manage, and maintain. Furthermore, it is difficult to comprehend the complex interdependencies that exist between information gathered from large and diverse sources for a system to be compliant with DITSCAP. To deal with such issues, the DITSCAP automation framework outlines an integrated, well-defined and comprehensive framework which combines novel techniques from requirements engineering and knowledge engineering. The framework supports 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 information system working as a whole, under a certain configuration in the given complex environment.

An integral part of the DITSCAP automation framework is Problem Domain Ontology (PDO) that provides the definition of a common language and understanding through the application domain concepts, properties and their relationships in the universe of discourse i.e. the DITSCAP domain. The DITSCAP PDO contains machine understandable hierarchical organization of ontological concepts with related properties and non-taxonomic dependencies among each other, to represent and structure the knowledge captured from the DITSCAP domain. The PDO is built and accumulated in a specialized module built upon the GENeric Object Model (GenOM) [12], which is an integrated development environment for ontological engineering processes with functionalities to create, browse, access, query and visualize associated knowledge-bases. To assist the C&A process, the DITSCAP PDO captures various dimensions of the DITSCAP problem domain through 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 non-taxonomic links between related risk sources; 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.

We now briefly discuss some important representations in the DITSCAP PDO that help to outline a risk assessment process in the later sections of the paper. More details about various models in the DITSCAP PDO can be found in [11].

3.1. The 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 with generic high-level Federal laws, mid-level DoD policies, and leaf-node site-specific security requirements. Using such inherent organization of documents, we create a hierarchical representation of ontological concepts derived from DITSCAP-oriented security requirements, carefully extracted and annotated with several attributes to form a Requirements Domain Model (RDM). Also, there exists several non-taxonomic links associated with security requirements in the RDM that represent relationships within the RDM as well as with other entities in the PDO. The ontological concepts of the RDM are then instantiated in the leaf-nodes of the hierarchy with site-specific security requirements.



Access to Need-to-Know Information
Only individuals who have a valid need-to-know that is demonstrated by assigned official Government duties.

Least Privilege
Access procedures enforce the principles of separation of duties and "least privilege."

Maintenance Personnel
Maintenance is performed only by authorized personnel.

Account Access Control
A comprehensive account management process is implemented.

Privileged Account Control
All privileged user accounts are established and administered in accordance with a role-based access scheme.

Enclave Boundary Defense
Include IDS and firewall at key points in the enclave

Encryption for Data in Transit
Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography

Key Generation
Cryptographic key should be generated based on a particular standard

Key Access
Specify the method used for cryptographic key backup, recovery, archive and storage

Key Distribution
Key distribution should be done based on an assigned standard

Figure 1 : Partial Example Requirements Domain Model

A partial RDM related to the Federal-level requirements for a 'security plan for information systems' is shown in Figure 1, which elaborates on Personnel Controls, Logical Access Controls, Network Controls and Cryptographic Controls, in its leaf-nodes. 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 requirements to be achieved by the system into a set of specific applicable requirements from DITSCAP-oriented 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.

3.2. The DITSCAP C&A Goal Hierarchy

In order to guide the systematic exploration of the RDM, the goals of the DITSCAP process are extracted from homogenous groupings of well-defined tasks and activities in [4] to create a hierarchical representation of the overall C&A process aspect knowledge. 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 the DITSCAP automation tool [13] users using wizard-based interfaces. A part of such a goal hierarchy is shown in Figure 3. The C&A goal hierarchy also identifies a space of applicable requirements through the mappings between the goals and the requirements in the RDM at the level of corresponding abstractions. Furthermore, the specific criteria gathered through leaf-node questionnaires help to prune or expand the search space identified by the goals over the RDM.

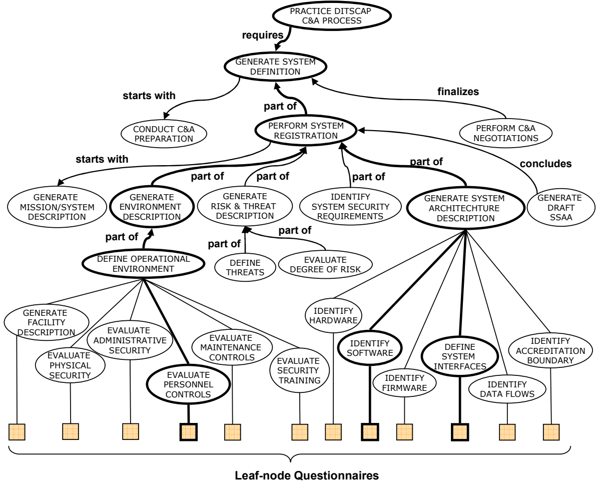

PRACTICE DITSCAP C&A PROCESS
requires
GENERATE SYSTEM DEFINITION
starts with
finalizes
part of
CONDUCT C&A PREPARATION
PERFORM SYSTEM REGISTRATION
PERFORM C&A NEGOTIATIONS
starts with
part of
part of
part of
part of
concludes
GENERATE MISSION/SYSTEM DESCRIPTION
GENERATE ENVIRONMENT DESCRIPTION
GENERATE RISK & THREAT DESCRIPTION
IDENTIFY SYSTEM SECURITY REQUIREMENTS
GENERATE SYSTEM ARCHITECHTURE DESCRIPTION
GENERATE DRAFT SSAA
part of
part of
part of
DEFINE OPERATIONAL ENVIRONMENT
DEFINE THREATS
EVALUATE DEGREE OF RISK
GENERATE FACILITY DESCRIPTION
EVALUATE ADMINISTRATIVE SECURITY
EVALUATE PHYSICAL SECURITY
EVALUATE PERSONNEL CONTROLS
EVALUATE MAINTENANCE CONTROLS
EVALUATE SECURITY TRAINING
IDENTIFY HARDWARE
IDENTIFY SOFTWARE
IDENTIFY FIRMWARE
DEFINE SYSTEM INTERFACES
IDENTIFY DATA FLOWS
IDENTIFY ACCREDITATION BOUNDARY
Leaf-node Questionnaires

Figure 3: Partial DITSCAP C&A Goal Hierarchy

3.3. DITSCAP Risk Assessment Taxonomy

The DITSCAP PDO also includes a risk assessment taxonomy that aggregates a broad spectrum of possible categories and classification of risk related information in the DITSCAP domain. The risk assessment concepts expressed in the higher level non-leaf nodes of this taxonomy can be achieved using specific criteria addressed in their leaf nodes. 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

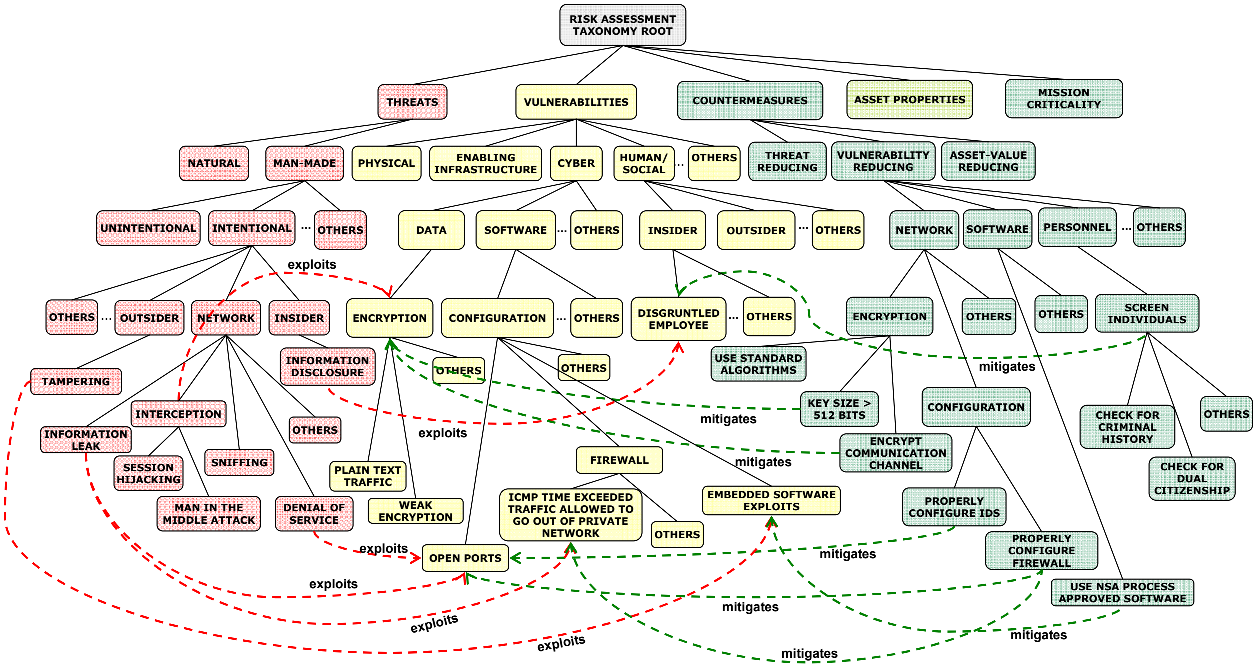


Figure 2: Partial DITSCAP Risk Assessment Taxonomy

risk assessment taxonomy in the upper level non-leaf nodes consists of threat, vulnerabilities, countermeasures, mission criticality, asset and other categories related to risk assessment. Each non-leaf node is then decomposed into more specific categories. Furthermore, the non-taxonomic links that exist between the categories of the taxonomy are critical to understand the relationships/dependencies between various risk factors. A partial DITSCAP risk assessment taxonomy is shown in Figure 2.

Similar to other models of the DITSCAP PDO the categorization and classification of the risk assessment taxonomy is based on the information sources available in the DITSCAP domain. We currently restrict its scope to the DITSCAP Application Manual [4]; the DITSCAP Minimal Security Checklists [4]; other DITSCAP-oriented directives and security requisites.

In the following sections, we demonstrate how the interactions between different models in the DITSCAP PDO contribute to an effective and comprehensive risk assessment in the DITSCAP. We now uncover the mappings that exist between security requirements and the associated risk factors to facilitate a mutual dialogue between them.

4. Security Requirements and Risk Factors

The DITSCAP PDO due to its ontological characteristics increases the cohesiveness of information between various system models and provides inherent properties of an active approach to link them via application domain concepts, properties and their relationships. Naturally, such a PDO can utilize the relationships that exist between security requirements and risk factors associated with an information system to drive a comprehensive risk assessment process. In Figure 4, we identify such relationships using a self-explanatory UML type notation. We extend the security model of Common Criteria standard [3] to incorporate security requirements and its relationships with the risk factors required to be considered in risk assessment. The model provides a baseline to comprehend security requirements from the viewpoint of the major factors in risk assessment. On the other hand, from a risk assessment perspective, a comprehensive collection of risk related information can be made available through security requirements, which can be used to drive an early cost-benefit analysis.

In the context of DITSCAP automation framework, the model in Figure 4 guides the generation of questionnaires that assess the compliance of security requirements in the leaf-nodes of the RDM. This step essentially relates security requirements to various risk factors in the risk assessment taxonomy. Furthermore, the non-taxonomic links in the RDM as well as the risk assessment taxonomy can be used to further identify and elaborate the concepts necessary for a comprehensive risk assessment. These aspects become evident as we discuss them with examples in the following section.

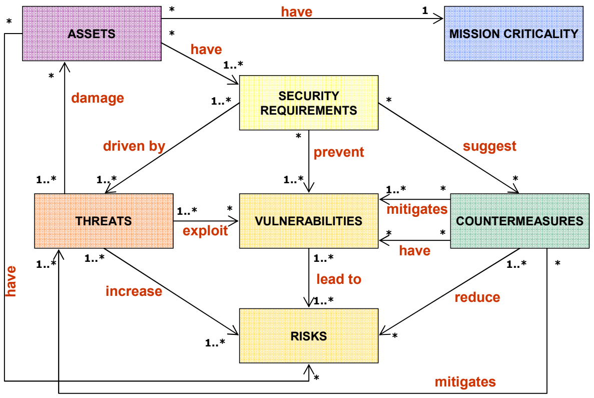


Figure 4: Security Requirements and Risk Relationship Model

5. Security Requirements Driven Risk Assessment in the DITSCAP

To demonstrate the risk assessment process in the DITSCAP automation framework we use examples based on the information system shown in Figure 5.

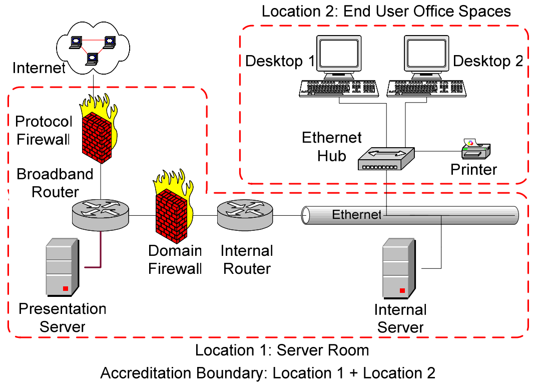


Figure 5: Example Information System

The example system is a web hosting site that makes available DoD policies and procedures on the internet for public access. To identify the DITSCAP-oriented security requirements applicable to this system, user/system criteria are gathered through the leaf-node questionnaires of the DITSCAP C&A goal hierarchy as shown in Figure 3. The gathered information helps to prune or expand the applicable requirements space projected over the RDM by the goals in the hierarchy. Figure 6 shows the user criteria captured in the leaf-node questionnaires of the goal paths highlighted in Figure 3. The scope of the questionnaires is based on the accreditation boundary, shown in Figure 5, which can be further divided into different physical locations of the system.

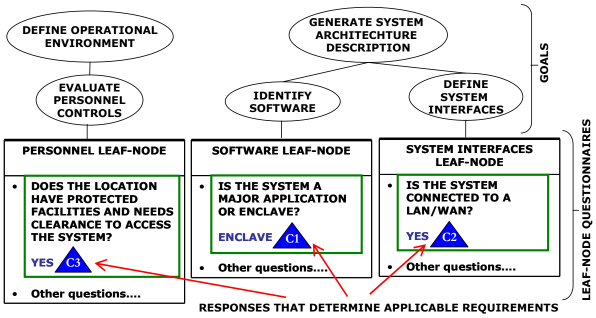
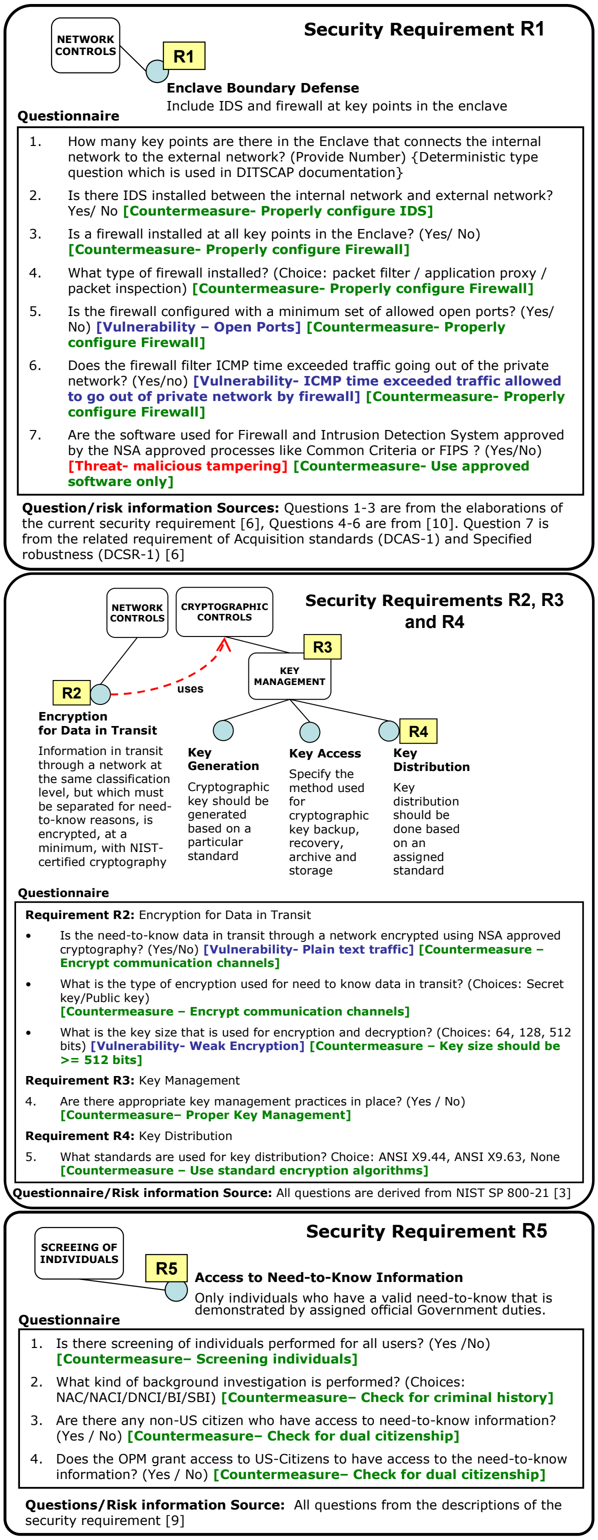

DEFINE OPERATIONAL ENVIRONMENT
GENERATE SYSTEM ARCHITECHTURE DESCRIPTION
EVALUATE PERSONNEL CONTROLS
IDENTIFY SOFTWARE
DEFINE SYSTEM INTERFACES
GOALS
PERSONNEL LEAF-NODE
SOFTWARE LEAF-NODE
SYSTEM INTERFACES LEAF-NODE
DOES THE LOCATION HAVE PROTECTED FACILITIES AND NEEDS CLEARANCE TO ACCESS THE SYSTEM?
YES
C3
Other questions....
IS THE SYSTEM A MAJOR APPLICATION OR ENCLAVE?
ENCLAVE
C1
Other questions....
IS THE SYSTEM CONNECTED TO A LAN/WAN?
YES
C2
Other questions....
LEAF-NODE QUESTIONNAIRES
RESPONSES THAT DETERMINE APPLICABLE REQUIREMENTS

Figure 6: Example Goal Hierarchy Questionnaires

The specific responses to the questions in Figure 6 (the triangular markers C1, C2 and C3) relate to corresponding nodes in the RDM of Figure 1, where they are used to prune or expand the set of applicable security requirements. The responses in Figure 6 bring into focus several categories of security requirements related to personnel controls, logical access controls, network controls and cryptographic controls from the partial RDM of Figure 1. Once the applicable set of security requirements has been identified, their compliance information needs to be gathered. The security requirements and risk relationship model as shown in Figure 4 helps in systematically guiding the discovery of such compliance information. In the DITSCAP domain, the relationships between security requirements and other elements in the model of Figure 4 are identified from various sources associated with the security requirements such as their descriptions/elaborations, research literature, taxonomies or from domain experts. These relationships are then made explicit in the form of questionnaires which are used to assess the level of compliance of security requirements of the RDM. These questionnaires, the risk factors addressed by them, and their sources for security requirements marked with rectangular markers R1 to R5 in the RDM of Figure 1, are shown in Figure 7.

The risk factors identified through this approach are as varied and diverse as the security requirements enforced by DITSCAP. But, it should be noted that security requirements do not always convey all risk related information. To address this issue, the non-taxonomic relationships that exist between various risk elements in the risk assessment taxonomy (Figure 2) can be used to identify the missing pieces of risk information for security requirements. For the example system under consideration, using the non-taxonomic relationships available from the partial risk assessment taxonomy in Figure 2, we identify additional risk information for the security requirements R1, R2 and R5 in Figure 8.



Enclave Boundary Defense
Include IDS and firewall at key points in the enclave

Questionnaire

1. How many key points are there in the Enclave that connects the internal network to the external network? (Provide Number) {Deterministic type question which is used in DITSCAP documentation}
2. Is there IDS installed between the internal network and external network? Yes/ No **[Countermeasure- Properly configure IDS]**
3. Is a firewall installed at all key points in the Enclave? (Yes/ No) **[Countermeasure- Properly configure Firewall]**
4. What type of firewall installed? (Choice: packet filter / application proxy / packet inspection) **[Countermeasure- Properly configure Firewall]**
5. Is the firewall configured with a minimum set of allowed open ports? (Yes/ No) **[Vulnerability – Open Ports]** **[Countermeasure- Properly configure Firewall]**
6. Does the firewall filter ICMP time exceeded traffic going out of the private network? (Yes/no) **[Vulnerability- ICMP time exceeded traffic allowed to go out of private network by firewall]** **[Countermeasure- Properly configure Firewall]**
7. Are the software used for Firewall and Intrusion Detection System approved by the NSA approved processes like Common Criteria or FIPS ? (Yes/No) **[Threat- malicious tampering]** **[Countermeasure- Use approved software only]**

Question/risk information Sources: Questions 1-3 are from the elaborations of the current security requirement [6], Questions 4-6 are from [10]. Question 7 is from the related requirement of Acquisition standards (DCAS-1) and Specified robustness (DCSR-1) [6]

Encryption for Data in Transit
Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography

Key Generation
Cryptographic key should be generated based on a particular standard

Key Access
Specify the method used for cryptographic key backup, recovery, archive and storage

Key Distribution
Key distribution should be done based on an assigned standard

Questionnaire

Requirement R2: Encryption for Data in Transit

- Is the need-to-know data in transit through a network encrypted using NSA approved cryptography? (Yes/No) **[Vulnerability- Plain text traffic]** **[Countermeasure – Encrypt communication channels]**
- What is the type of encryption used for need to know data in transit? (Choices: Secret key/Public key) **[Countermeasure – Encrypt communication channels]**
- What is the key size that is used for encryption and decryption? (Choices: 64, 128, 512 bits) **[Vulnerability- Weak Encryption]** **[Countermeasure – Key size should be >= 512 bits]**

Requirement R3: Key Management

4. Are there appropriate key management practices in place? (Yes / No) **[Countermeasure– Proper Key Management]**

Requirement R4: Key Distribution

5. What standards are used for key distribution? Choice: ANSI X9.44, ANSI X9.63, None **[Countermeasure – Use standard encryption algorithms]**

Questionnaire/Risk information Source: All questions are derived from NIST SP 800-21 [3]

Access to Need-to-Know Information
Only individuals who have a valid need-to-know that is demonstrated by assigned official Government duties.

Questionnaire

1. Is there screening of individuals performed for all users? (Yes /No) **[Countermeasure– Screening individuals]**
2. What kind of background investigation is performed? (Choices: NAC/NACI/DNCI/BI/SBI) **[Countermeasure– Check for criminal history]**
3. Are there any non-US citizen who have access to need-to-know information? (Yes / No) **[Countermeasure– Check for dual citizenship]**
4. Does the OPM grant access to US-Citizens to have access to the need-to-know information? (Yes / No) **[Countermeasure– Check for dual citizenship]**

Questions/Risk information Source: All questions from the descriptions of the security requirement [9]

Figure 7: Questionnaires for Security Requirements in the RDM Leaf nodes

The relationships between security requirements and the risk categories in Figure 8 are not static but they can be dynamically discovered and reconfigured based on the user/system criteria and other information as it becomes available in the environment. Moreover, the risk categories can now be evaluated in the context of security requirements that naturally capture the complex relationships between system components as well as the environment.

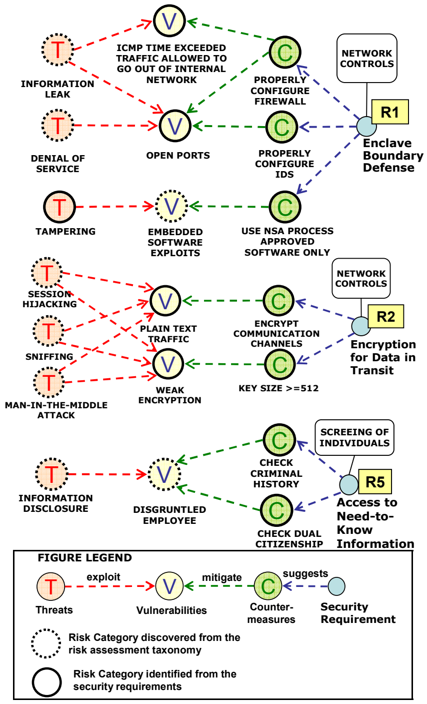


Figure 8: Elaboration of the Risk factors identified for Security Requirements

As we systematically identify the threats, vulnerabilities and countermeasures applicable to the system from various dimensions, for an effective risk assessment it is also essential to identify the "*necessity*" and "*sufficiency*" of these risk factors in addressing each other. For example, if the countermeasures related to a vulnerability are "*necessary*" then the risk associated with that vulnerability is not mitigated unless all the required countermeasures are satisfied. Additionally, if a countermeasure is considered "*sufficient*" for a vulnerability and if that countermeasure is satisfied then the absence of other related countermeasures does not escalate the risk related to that vulnerability. Similar properties also need to be identified for the relationships between threats and vulnerabilities. Based on such criteria, sets of closely-related threats, vulnerability and countermeasures can be created to further identify the dependencies between various risk categories in the risk assessment taxonomy. Moreover, in order to perform a cost-benefit analysis for establishing *adequate security*, the security requirements can be prioritized based on metrics established through such closely-related sets, for example, the collective density of the related threats, vulnerability and countermeasures or their individual densities. Such metrics should also take into account the capabilities of the assets being protected and their associated mission criticality. The metrics and measures developed in this manner help to identify and lead to carefully designed security requirements, as well as bring additional attention to those requirements that face high risks and thus require enforcing additional security requirements on the system.

6. Related Work

In the information security domain, the Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) [2] criteria provides the definition of a general approach for evaluating and managing information security risks. But OCTAVE relies on the organization to develop their own methods to satisfy its criteria. The CORAS [1] project advocates a UML based approach for risk assessment but their focus is to combine several methods and standard of risk assessment. In [24] Vaughan et al. identify that information assurance metrics are usually specific to an organization and depend on their technical, organizational and operational needs and the resources they can make available. We believe that in order to promote consistency between the IA standards and their real world interpretations and implementations it is necessary to promote a common understanding and traceability at different levels of abstraction [10].

In the early and late requirements engineering stages, several approaches exist to identify illicit usage or threat scenarios using misuse/abuse cases [20], abuse frames [15], intruder anti-goals [23], or attacker modeling and analysis [14], exist but they only uncover a limited set of threats based on the current context of analysis.

In [8] Freeman et al. outline several essential characteristics of a risk assessment methodology for large heterogeneous systems. Based on these characteristics, we believe that the DITSCAP automation framework provides a good setting for practicing risk assessment for systems in the DII.

7. Conclusion

Our contributions in this paper can be summarized as follows. Firstly, by identifying the shortcomings of the current approaches to perform C&A, we motivate the necessity of several modeling techniques to adequately understand the complexity of information systems and their socio-technical operational environments. Secondly, we outline the relationships that exist between security requirements and the elements of risk assessment to systematically support the interactions between various models defined in the DITSCAP automation framework. These relationships help in conducting an objective, repeatable and justifiable risk assessment driven by security requirements based on the links established between the artifacts captured through the RDM and the risk assessment taxonomy. However, it should be noted that risk information in the DITSCAP automation framework can be gathered from several different dimensions such as user/system criteria, viewpoints of the stakeholders, the real-world goals and objectives, business/mission requirements, regulatory requirements, or specific operational scenarios. When these different pieces of information finally come together, they form *valuable knowledge* that helps to understand the complex interdependencies and causal chains that exist between the real world goals, objectives and the components of the system undergoing C&A. Also, such analysis will evolve as more information becomes available from the environment, which is in turn used to guide the decisions made for the system throughout its lifecycle in a predictable manner.

Our future and on-going work include the creation of an advanced risk calculation algorithm that leverages the ontological characteristics of the DITSCAP PDO to gather information from several sources. Such an algorithm should communicate its results at various levels of abstractions and consider diverse viewpoints to effectively drive the negotiations between stakeholders. The DITSCAP automation framework also offers an opportunity to establish several metrics and measures for risk assessment based on a common understanding and the reflected language from various dimensions of the DITSCAP PDO. Although we currently focus on the DITSCAP domain, our approach can easily scale to accommodate general dependability requirements, polices and practices in any domain of interests.

Acknowledgements: This work is partially supported by the grant (Contract: N65236-05-P-2418) 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, Divya Muthurajan, Raghuram Gururajan, and Swapnil Brahmankar for their contributions.

8. References

[1] Aagedal, J.O., den Braber, F., Dimitrakos, T., Gran, B.A., Raptis, D., Stolen, K., “Model-based risk assessment to improve enterprise security,” In Proceedings of the 6th International Enterprise Distributed Object Computing Conference, 17-20 Sept. 2002 Page(s):51 - 62

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

[3] Common Criteria, Part 1: “Introduction and general model,” Version 2.1. ISO/IEC 15408-1, August 1999.

[4] DoD 8510.1-M, “DITSCAP Application Manual”, 2000.

[5] DoD Instruction 5200.40, “DITSCAP”, 1997

[6] DODD 5200.2-R DoD Personnel Security Program, 1987

[7] DoDI 8500.2, “Information Assurance Implementation”, 2003.

[8] Freeman, J. W., Darr, T. C., & Neely, R. B., “Risk assessment for large heterogeneous systems”, In Proceedings of the 13th Annual Computer Security Applications Conference, 1997, pp: 44

[9] Lee, A., “A Guideline for implementing cryptography in the Federal government,” NIST SP 800-21, November 1999.

[10] Lee, S. W., and Gandhi, R. A., “Engineering Dependability Requirements for Software-intensive Systems through the Definition of a Common Language”, To Appear in the Proceeding of Requirements for High Assurance Systems Workshop (RHAS '05), RE 2005, August 2005

[11] Lee, S. W., Gandhi, R. A., & Ahn, G, “Establishing Trustworthiness in Services of the Critical Infrastructure: Automating the DITSCAP”, Workshop on Software Engineering for Secure Systems (SESS05), 27th International Conference on Software Engineering (ICSE 05), May 2005

[12] Lee, S.W. and Yavagal, D. GenOM User’s Guide. Technical Report TR-SIS-NISE-04-01, UNC Charlotte, 2004

[13] Lee, S.W., Ahn, G. and Gandhi, R.A. “Engineering Information Assurance for Critical Infrastructures: The DITSCAP Automation Study.” In Proceedings of the 15th Annual INCOSE, Rochester, NY, July 10-15. 2005.

[14] Liu, L., Yu, E., Mylopoulos, J., “Security and privacy requirements analysis within a social setting”, In proceedings of 11th IEEE International RE Conference, 2003, pp: 151-161

[15] Luncheng Lin, Nuseibeh, B., Ince, D., Jackson, M, “Using abuse frames to bound the scope of security problems”, In Proceeding of the 12th IEEE Int’l Requirements Engineering Conference, 2004, pp: 354- 355

[16] NIST-SP 800-12, “An Introduction to Computer Security: The NIST Handbook,” October 1995

[17] OMB Circular No. A-130, “Management of Federal Information Resources,” Feb 8 , 1996

[18] P. L. 100-235, “Computer Security Act of 1987,” 1998

[19] Press release, http://reform.house.gov, “Davis Statement on 2004 Federal Computer Security Report Card Grades”

[20] Sindre, G., Opdahl, A.L., “Eliciting security requirements by misuse cases”, In Proceedings of the 37th Int’l Conference on Technology of OO Languages and Systems, 2000, pp:120-131

[21] Skoudis, E., *Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses,* PrenticeHall, 2001

[22] System Security Engineering Capability Maturity Model Description Document. Version 3.0. June 15, 2003

[23] van Lamsweerde, A., Brohez, S., De Landtsheer, R., and Janssens, D., “From System Goals to Intruder Anti-Goals: Attack Generation and Resolution for Security Requirements Engineering” In Proceeding of Requirements for High Assurance Systems Workshop (RHAS'03), 2003

[24] Vaughn, R.B., Henning, R. and Siraj, A. “Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy.” In Proceedings of the 36th Annual Hawaii International Conference on System Sciences, pp: 331- 340, 2003