Utilizing the Common Criteria for Advanced Student Research Projects

Thuy D. Nguyen and Cynthia E. Irvine

Naval Postgraduate School, Monterey, CA 93943, USA
{tdnguyen,irvine}@nps.edu

Abstract. In most computer science graduate programs, students must complete an advanced research project that demonstrates the students technical competence in both the theory and practice of the field. Information security is a specialization area of computer science whose research results have direct benefits to real world problems. The Common Criteria (CC) is an international standard for security evaluation of products. This paper describes the utilization of the CC paradigmatic framework for advanced student research projects focused on security engineering. Three CC-based efforts of varying levels of difficulty are presented and the suitability and benefits of applying the CC in this context are discussed.

1 Introduction

Information security is a specialization area of computer science that is increasingly attracting attention of academic, government, and industry-based communities. This interest is driven by the exploitability of the Internet and the heightened awareness of the lack of assurance in commodity computers. Although work in computer security has been ongoing for several decades, it has not been adopted along with other rapid advances in computer and network technologies. This gap stems from the fact that the commercial sector is under constant pressure to reduce time-to-market and compete with the latest technical gimmicks. Thus, the commercial sector has tended to ignore the principles [1] and fundamentals of information security in product development. Accelerating government and commercial adoption of emerging technologies has created significant financial and national security risks that must be addressed.

While the academic community has been more proactive in addressing the need for better security education to prepare students for the real world workplace [2], typical computer security coursework often tends to focus on static code analysis, cryptography, secure protocols, and intrusion detection and analysis. The security track of the Computer Science (CS) department at our institution incorporates additional disciplines in information assurance and security with an emphasis on high assurance secure systems and security engineering.

The Common Criteria (CC) is an internationally-recognized set of criterions for Information Technology (IT) security evaluation [3]. It is the result of a multinational effort to harmonize different security evaluation criteria independently

developed by several North American and European governments [4–6]. As the use of the CC in the commercial sector becomes more widespread, a natural progression would be to use it in education and research to both prepare students for proficiency in secure system and software engineering techniques and to nurture their appreciation of the value of rigorously-developed secure systems. CC hegemony remains an uncertain prospect, but the pedagogical value of applying the CC to information security education and research is clear. Our premise is that if the CC framework and methodology are used in both instructional courses and student research projects, the students understanding of the fundamental principles of information security will be more effectively strengthened and the quality of student work will improve quantitatively. The central notion is that this holistic approach enables the students to become better practitioners of the fundamental knowledge gained during their academic endeavor.

This paper describes how the CC was utilized as a practical tool for security requirements derivation in advanced student research projects. Background information on CC coursework and information security research projects is presented, followed by the description of three thematic projects guided by the CC framework. A discussion of the experience with the CC-based research approach is included.

2 Background

Our nascent framework on CC education combines both traditional coursework and faculty-supervised student theses that are part of multi-year research efforts.

2.1 Information Assurance Courses

The computer science (CS) coursework portfolio in our department consists of a set of core computer science classes and a number of specialization courses. The information assurance and security track augments the core CS classes with principles and techniques of developing secure systems [7]. The CC concepts and goals covered in some of the security track courses are described in Table 1.

2.2 Information Security Research Projects

Trusted Computing Exemplar (TCX) Project. The TCX project provides an openly disseminated worked example of how high robustness trusted components can be constructed. The CC plays a crucial role, since the project reference implementations, the TCX Separation Kernel and Trusted Path Extension application, are targeted for the CC Evaluation Assurance Levels 7 and 6 (EAL7 and EAL6), respectively [8, 9].

The security requirements (both functional and assurance) for the TCX kernel will be based on the Separation Kernels Protection Profile (SKPP) [10]. Although the TCX team has considerable previous experience in high assurance development, our participation in the authoring of the SKPP provides a

different perspective on the process to produce secure software and systems. Specifically, we have found that with its iterative requirements derivation process and structured requirements specification methodology, the CC can also be used to effectively capture requirements for software and systems that are not intended to undergo formal evaluation.

Table 1. CC Coverage in IA Courses

Course	Common Criteria Coverage
CS3600 Introduction to Information Assurance: Computer Security	This class offers an introductory overview of the CC taxonomy, basic concepts in requirements specification and security evaluation, Evaluation Assurance Levels, and evaluation methodology for government-certified evaluation labs.
CS3670 Information Assurance: Secure Management of Systems	This class teaches secure system administration and management and discusses requirements covered in CS3600 in the context of DoD policies and national standards (e.g., NIST publications).
CS4600 Secure Systems	This class addresses the principles and techniques of high assurance secure system development. It includes a CC-based laboratory project that introduces the students to the CC methodology and assurance requirements. The students learn how to apply in the CC framework in projects such as requirements formulations and security extensions to an existing operating system.
CS4614 Advanced Topics in Computer Security	This class discusses academic papers on advanced topics in computer security, including the CC interpretation process and the notion of high assurance composite evaluation. The students gain exposure to how the CC standard process is driven at the national level and the needs to improve the CC methodology to support high assurance composite evaluations.
CS4680 Introduction to Certification and Accreditation	This class provides an introduction to the Certification and Accreditation (C&A) process as applied to government systems. The CC fundamentals covered in CS3600 are iterated in the context of C&A, with emphasis on hierarchical Evaluation Assurance Level differences.

Monterey Security Architecture (MYSEA) Project. The MYSEA project establishes an overarching framework that facilitates research and experimenta-

tion with ergonomic, i.e., user-centric, multilevel security (MLS). MYSEA is a client-server distributed network environment that comprises a federation of high assurance MLS servers and a number of local and remote networks of both security-enhanced and unmodified commercial off-the-shelf clients [11, 12]. The MYSEA server enforces the overall system security policy and its trusted operating base recently completed a CC EAL5 evaluation [13]. The security-enhanced client system consists of a specialized security appliance (named Trusted Path Extension) and commodity PCs executing popular commercial software. The Trusted Path Extension provides user authentication and access control support mechanisms, and the TCX Kernel will be used as its trusted operating base.

Although the provenance of MYSEA can be traced back to the TCSEC, recent and current research activities are based on the CC framework. The CC paradigm of defining secure systems in terms of the desired assurance level and security capability, and against a well-defined threat analysis has been successfully adopted for use in a number of MYSEA-related student projects.

Multilevel Print Server (MPS) Project. The MPS project is part of a network-centric information assurance solution that provides secure sharing of network resources across different security domains. The goal of the MPS project is the design and development of a trusted print server that can securely separate print jobs originating from networks operating at different security levels. Since the MLS print server is targeted for a CC evaluation at EAL4-plus, i.e., EAL4 with augmentation, the initial project goal is to develop a CC protection profile (PP) sketch that defines the necessary set of security requirements at that level for the MLS print server. The PP sketch was originally developed using Version 2.2 of the CC and is now being transitioned to Version 3.0 of the CC [14]. To achieve Version 3.0,the CC underwent a major overhaul and a significant amount of effort is required to fully understand the ramifications of the changes. The lack of requirements regarding hardware assurance, trusted initialization, and the application of the principle of least privilege to both internal functions and external subjects (e.g., programs) is a notable omission.

3 Theses as Case Studies in Common Criteria Application

A number of advanced student research projects have emanated from the above research efforts. Completing a thesis that demonstrates the students mastery in both core and specialized subjects acquired through course work is a curriculum requirement for all students. Three theses are described here to illustrate the effectiveness of applying the CC framework to student research. The CC affords students a systematic means to organize and conduct information security research with different levels of difficulty. It also provides the thesis advisors with quantitative metrics to assess the research result. Qualitative assessment of the students ability to perform independent, graduate level research is subjective. However, the students technical strength can be partially determined based on

the students ability to navigate and articulate the large selection of security requirements defined by the CC.

In the sections that follow three theses are examined. These theses were selected based on the extent of their CC utilization, the difficulty level of the research project, and the students research ability. Table 2 summarizes the project characteristics. In all cases, the students were expected to apply analytical reasoning skills and graduate level research techniques to their work.

Table 2. Project Characteristics

Project	CC Utilization	Difficulty Level	Student Ability
TCX Dissemination System	Informally defined requirements; low robustness	Low	Above average
MYSEA Single Sign-On Framework	Informally defined requirements; medium robustness	Medium	Excellent
MLS Print Server Protection Profile Sketch	Formally defined requirements; medium robustness	High	Above average

3.1 TCX Dissemination System

Open dissemination of project material is one of the core objectives of the TCX project. For TCX, open dissemination does not mean unrestricted dissemination. TCX materials have access control markings that are used as the basis for distribution by the dissemination system [15].

The design of the TCX dissemination system is a worked example of the application of the CC methodology to derive and express security requirements for an informally specified system. The research activities for this effort can be logically separated into three stages: system requirements elicitation, security requirements derivation, and proof-of-concept prototype implementation. The CC plays an important role in the second stage.

Based on the threat properties of the TCX dissemination system, e.g., a web interface that is to be available online to the general public, a threat analysis of the trusted delivery mechanisms required for the TCX kernel was completed first. The result of this analysis helped narrow down the list of high level system requirements for the dissemination system. In contrast with the next stage where the use of the CC is prominent, the requirements elicitation process was conducted informally.

In the second stage, a CC-based requirements derivation process was used to translate, through structured analysis, the high level system requirements into a set of informal security requirements for both the dissemination system and its environment. The CC requirements expression rules were loosely followed to help organize and represent these security requirements. A number of improperly specified objectives and requirements were discovered and redefined as the result of iteratively applying the CC traceability methodology. The last stage involved the construction of an initial implementation that satisfies a subset of the system requirements.

In the U.S. evaluation scheme, the robustness level of a system is determined by the value of the resources that the system needs to protect and the authorization of external entities that can access the resources [16]. A basic level of robustness was selected for the dissemination system because the project materials that can be disseminated online are low-value data, reducing the likelihood of attacks by external entities (i.e., Internet users). High-value project materials are handled separately, on a case-by-case basis.

Although the CC requirements derivation process was used, the difficulty level of this thesis is rated low because the requirements need not be stated with CC constructs. Furthermore, the design of the dissemination system was from a clean slate, with no backward compatibility burdens. However, due to the students steep learning curve on both the CC and the web technology required to implement the initial prototype, the thesis took longer than expected to complete.

3.2 MYSEA Single Sign-On Framework

To address scalability, the MYSEA design allows the use of more than one MYSEA server in a local operating environment. Support for such a federation of servers is not available in the current MYSEA implementation. To avoid requiring the user to separately authenticate to different servers, a secure single sign-on user authentication mechanism is needed. Hence, the primary objective of this student research project is to define an architectural framework and high level design for a single sign-on (SSO) solution for MYSEA [17].

Central to the SSO design is the MYSEA Authentication Server. One of the MYSEA servers in the federation will assume this role and be responsible for user authentication and session negotiation. The other SSO component is the MYSEA Application Management Server. This component provides application services to authenticated users and can colocate with the authentication server on the same platform. Although the SSO design allows the Authentication Server functionality to be distributed among multiple servers, the thesis focused primarily on the single Authentication Server configuration. The security, usability, and to a lesser extent, performance and reliability requirements of the Authentication Server were within the scope of this thesis.

Similar to the TCX dissemination system project, the decision to use the CC as a guiding tool for security analysis was made early in the thesis process. The CC methodology for defining security requirements based on threats, security

assumptions, organizational security policies, and security objectives in the context of a protection profile was applied to develop security requirements for the Authentication Server component. Security analysis of the Application Management Server component and the distributed Authentication Server configuration were identified as future work.

Ideally the robustness level of the Authentication Server should be high since the MYSEA network is an MLS environment. However, medium robustness was chosen for this thesis for three reasons: 1) guidance for high robustness PP development is currently not available, 2) other than the emerging SKPP there were no existing high assurance protection profiles that the student could examine for reference, and 3) the work had to be at an attainable level so that the student could complete within the time allotted for thesis work.

The difficulty level of this thesis was expected to be medium because the SSO design was required to fit into the existing MYSEA architecture. Furthermore, security analysis of a distributed architecture is complex, especially when the use of structured security evaluation criteria is imposed on the analysis. The learning curve on the CC methodology was not as steep as in the case of the TCX dissemination system thesis (discussed earlier) since the dissemination system thesis was available for use as example. Not using the CC constructs and wording to express the security requirements also simplified the work.

3.3 MLS Print Server Protection Profile Sketch

A multilevel print server (MPS) enforces a mandatory access control policy regarding input received from multiple networks at different sensitivity levels, and provides trusted separation pages indicating the sensitivity level of print jobs sent to either a dedicated or networked system high printer. The MPS also enforces supporting policies to include: detection of malicious print jobs, audit generation, audit logging and alarms, a trusted path for administrators, security and audit administrator tools, and operator services. The thesis goal was to develop a necessary set of security requirements, in the context of an EAL4 (with augmentation) protection profile sketch, for an MPS supporting Hewlett Packard Print Command Language (PCL) [18].

In the case of this thesis, the difference between a PP sketch and a complete PP was the omission of the rationale sections. In the CC paradigm, a PP must provide rationale that explains how the security requirements satisfy the stated security objectives, and how the objectives mitigate the threats and implement the organizational policies. Writing a comprehensive rationale is difficult and it was determined a priori that it would be an unachievable goal for the student.

Multiple factors distinguished this student project from the last two. It was our first experiment involving students in structured CC work in the form of a protection profile sketch. The PP sketch was developed to address a real-world security need and had to satisfy specific system requirements established by the intended users. Last, the PP sketch required structured expression of security requirements that conform to the Consistency Instruction Manual for PP development [19]. The thesis difficulty level was high due to these factors.

This thesis is highly technical because it requires a good understanding of the CC, multilevel security, component composition, and PCL printer technology. These prerequisites together with the students steep learning curve necessitated extensive faculty involvement in order to complete the project on time.

4 Discussion

For the theses examined, the CC security analysis methodology was an effective tool for analyzing and deriving security requirements. However, the suitability of the CC for non-instructional education does not stop there. When used as an organizational framework in student research projects, the CC provides a structure for keeping the project goal in focus and making decisions, both technical and logistic. It also affords the thesis advisors a means to encourage students to employ self-governance of their work. Each student met weekly with the faculty advisors. A weekly goal emerged from each meeting. For example, students might be required to produce a certain section of their requirements document in the CC format, e.g., threats, assumptions, etc., prior to the next meeting at which a review of the work would be conducted. These reviews provided the student with feedback which either resulted in another iteration of the section or transition to a new section or phase of the effort.

4.1 Student Readiness

It became apparent that the CC-based approach was challenging and expensive for the faculty advisors since the CC learning curve was steep for the students. The CC coverage in the six core and specialized courses described earlier was not enough to prepare the students for CC-based research work. It has also become evident that classroom instruction on the CC must be reinforced by hands-on experience in order for the information learned from these classes to sink in.

4.2 Commonalities of Theses

The CC defines a system that undergoes evaluation as a Target of Evaluation (TOE) and a set of hardware and software mechanisms of the TOE that enforces the security policy as the TOE Security Functions (TSF) [3]. Although each thesis addressed a different TOE, all required the students to go beyond what they had learned of the CC in their classes.

First, each student had to define the system sufficiently to allow the identification of the TOE and its boundary. The use of the CC paradigm affords the student a systematic way to identify security critical functionality, resulting in a more precise system definition. As it was, each student had to identify elements of the system that were beyond the control of the TOE. They then had to determine the boundary of the TSF. As each system was in its conceptual stage, this process tended to be difficult and required considerable design discussion with the faculty advisors. What added to the challenge was the initial lack of intuition

on the part of the students regarding the distinctions among TOE, TSF, and the external components with which the TOE would interoperate.

Creation of the requirements creation was iterative and, for the students, this generally presented a challenge. Some were used to a very linear approach to problem solving that did not require adjustments. The thought of revisiting a stage that had already been addressed (often with the belief that the previous work at that stage was complete) seemed to be viewed as failure rather than an opportunity for improvement. Thus, the students needed to develop a new perspective to problem solving.

The CC-based process used by the students to derive security requirements is depicted in Figure 1. The process consisted of three iterative phases. In Phase I, the system description was prepared, starting with the general description of the thesis topic and followed by a series of refinements. The resulting system description covered different aspects of the target system, including its concept of operation, conceptual architecture and system access policy. Phase II involved the establishment of the security objectives. This was started with the definition of the systems security environment stated in terms of anticipated threats, environmental assumptions, and organizational security policies. The appropriate PP authoring manual [16, 19] was consulted to create the initial set of threats, assumptions, and organizational policies, which were then solidified through an iterative pruning and feedback process. A careful analysis of the security environment resulted in a set of security objectives that satisfied the intended functional goals and purpose of the target system. The articulation of the security requirements took place in Phase III. Depending on the nature of the thesis, the security requirements were specified either informally using an ad hoc format or formally using CC constructs and wording. The development of the requirements was also iterative and often caused subsequent reassessments of the security objectives.

The CC paradigm for requirements derivation is iterative by nature and requires the results of a given activity be traceable to the derived elements of the previous activity. The traceability is demonstrated by the evidential material defined as rationale description. In two theses, the rationale that mapped the threats, assumptions, and organizational policies to security objectives was produced. Each threat and organizational policy was mapped to an objective that addressed it and a rationale was provided for why that objective mitigated the threat. Assumptions were mapped to environmental objectives, with a corresponding rationale describing how the environmental objective met the assumption. Each security objective should have been mapped to one or more security requirements but this last set of mappings was not conducted.

There were several reasons for omitting the rational in the objectives-to-requirements mapping. Primary among them was the fact that the students simply ran out of time due to the steep learning curve they had experienced with the Common Criteria. In addition, we felt that their level of experience working with the Common Criteria was insufficient for that task. Thus, had we demanded that they prepare a rationale, it would have amounted to a mechani-

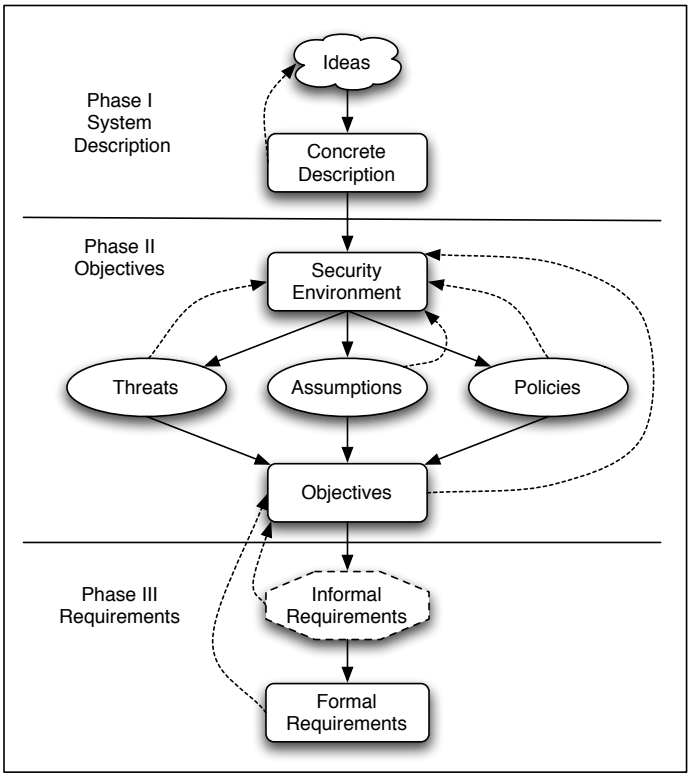

Fig. 1. Feedback cycles in requirements process

cal exercise for them and would not have contained the subtle observations that make the objectives-to-requirements rationale useful.

4.3 Faculty Experience

The advisors involved in the case study theses are well trained in both security engineering and security evaluation criteria. Our work on the SKPP provided valuable insights into how the CC works, which triggered the realization that the CC could be adapted for use in areas that traditionally do not require a structured framework. Since the CC is constantly being improved at both international and national levels, we have been concentrating mostly on the interpretations and guidance pertinent to the U.S. scheme. Our approach to keep abreast with the ever-changing CC is to actively participate the development of various protection profiles. Since the TCX kernel and reference applications are targeted for EAL 7 and EAL 6, we are further motivated to continue to stay on top of the latest CC developments.

5 Conclusion

The goal of this paper is to demonstrate that the use of the Common Criteria as a research framework for graduate students is beneficial as it imposes disciplines required for secure systems and software development on the research work. For thesis advisors, these disciplines help establish a trackable process to monitor student performance and progress.

To better prepare the students for CC-based research, we are currently developing a full-quarter course on the application of the Common Criteria for security analysis and engineering of secure systems and software. In addition to its primary objective, we intend for this course to provide an in-depth understanding of how security evaluation criteria can be adapted for use in non-evaluation activities, including academic research. Included in the course work is the examination of existing Protection Profiles and Security Targets which gives students both insight on domain-specific requirements expression and familiarity with the complicated CC-prescribed constructs and rules. It is anticipated that this hands-on approach will smooth out the students learning curve prior to thesis work, making it less demanding for both the student and thesis advisors.

We are continuing our experiment in this area with an in-progress thesis on the development of a high robustness PP sketch for a trusted platform. Since guidance for authors of high robustness protection profiles does not exist and the security issues associated with a high assurance platform that the PP sketch must address are highly complex, it remains to be seen if our approach will be as effective as in the past.

Related future work is to determine if requirements derivation would be easier if one could assume that it is possible to determine when a class of failures could be detected.

Acknowledgements

This work was sponsored in part by the Office of Naval Research, National Reconnaissance Office, and SPAWAR PMW-160. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsoring organizations.

References

1. Benzel, T. V., Irvine C. E., Levin, T. E., Bhaskara, G., Nguyen, T. D., Clark, P. C., Design Principles for Security, NPS Technical Report NPS-CS-05-010, September 2004.
2. Bishop, M., Frincke, D., Joining the Security Education Community, IEEE Security and Privacy Magazine, V. 2, No. 5, 2004, pp. 61 63.
3. Common Criteria for Information Technology Security Evaluation, Version 2.2, CCIMB-2004-01-[001, 002, 003], Common Criteria Project Sponsoring Organizations, January 2004.

4. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, National Computer Security Center, December 1985.
5. Canadian Trusted Computer Product Evaluation Criteria, Communications Security Establishment, Government of Canada, Canadian System Security Centre, Ottawa, Canada, January 1993.
6. Information Technology Security Evaluation Criteria, Office for Official Publications of the European Communities, Commission of the European Communities, Luxembourg, 1991.
7. Irvine, C., A Common Criteria-based Project for High Assurance Secure Systems, Proceedings of the IFIP TC 11 WG 11.8, 4th World Conference on Information Security Education, Moscow, Russia, May 2005, pp. 82-93.
8. Irvine, C. E., Levin, T. E., Nguyen, T. D., and Dinolt, G. W., The Trusted Computing Exemplar Project, Proc. IEEE Systems Man and Cybernetics Information Assurance Workshop, West Point, NY, June 2004, pp. 109-115.
9. Nguyen, T. D., Levin, T. E., and Irvine, C. E., TCX Project: High Assurance for Secure Embedded Systems, Proc. 11th IEEE Real-Time and Embedded Technology and Applications Symposium, Work in Progress Session, San Francisco, CA, March 2005, pp. 21-25. (Also appeared in SIGBED Review, Vol. 2, No. 2, April 2005, Special Issue on IEEE RTAS 2005 Work-in-Progress.)
10. U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness, Version 0.621, National Security Agency, 1 July 2004.
11. Irvine, C. E., Levin, T. E., Nguyen, T, D., Shifflett, D., Khosalim, J., Clark, P. C., Wong, A., Afinidad, F., Bibighaus, D., and Sears, J., Overview of a High Assurance Architecture for Distributed Multilevel Security, Proc. IEEE Systems Man and Cybernetics Information Assurance Workshop, West Point, NY, June 2004, pp. 38-45.
12. Nguyen, T. D., Levin, T. E., and Irvine, C. E., MYSEA Testbed, Proc. 6th IEEE Systems, Man and Cybernetics Information Assurance Workshop, West Point, NY, June 2005, pp. 438-439.
13. Common Criteria Evaluation and Validation Scheme Validation Report for BAE System Information Technology LLC XTS-400/STOP 6.1.E, Report Number: CCEVS-VR-05-0094, National Institute of Standards and Technology and National Security Agency, 1 March 2005.
14. Common Criteria for Information Technology Security Evaluation, Version 2.0 Revision 2, CCIMB-2005-07-[001, 002, 003], Common Criteria Project Sponsoring Organizations, June 2005.
15. Kane, D. R., Web-based dissemination system for the Trusted Computing Exemplar Project, Masters Thesis, Naval Postgraduate School, Monterey, CA, June 2005.
16. Consistency Instruction Manual For Development of US Government Protection Profiles For Use in Basic Robustness Environments, Release 3.0, National Security Agency, 1 February 2005.
17. Bui, S., Single Sign-on Solution for MYSEA Services, Masters Thesis, Naval Postgraduate School, Monterey, CA, September 2005.
18. Lysinger III, J. E., Multilevel Print Server Requirements for DoN Application, Masters Thesis, Naval Postgraduate School, Monterey, CA, June 2005.
19. Consistency Instruction Manual For Development of US Government Protection Profiles For Use in Medium Robustness Environments, Release 3.0, National Security Agency, 1 February 2005.