

CNSS Mapping for IA Lab Exercises

Ronald C Dodge JR, *United States Military Academy* and Helen Armstrong, *Curtin University*

Abstract – The number of tertiary institutions gaining recognition as a Center of Academic Excellence in Information Assurance has increased steadily since its inception. Although there is some debate on the desirability to align ‘university education’ with training standards and certifications, such recognition provides a baseline of skills and knowledge upon which the information security industry may rely. The task of developing IA curriculum to meet the needs of the standards compliance is a detailed and time-consuming task, with much duplication of effort across educational bodies. This paper presents the idea of using lab exercises to meet the needs of the CNSS standards, which form the basis of the CAEIA requirements and at the same time provide a meaningful and interesting learning experiences for the students..

Index terms – Laboratory Exercises, Information Assurance, Security Education, Standards

I. INTRODUCTION

The Center of Academic Excellence in Information Assurance (CAEIA) program is one where opinions vary as to its effectiveness. When viewed as a true measure of an institution’s stature of excellence it is thought by many to be lacking [1]. When viewed as a program to increase faculty participation and discussion and establish a baseline of experience for graduates entering a highly applied field, the CAEIA program has been immensely successful. As a foundation to ensure a common baseline for IA education it would be difficult to point to a more effective effort in any discipline. The purpose of this paper is not to contrast the opinions and fuel the debate, rather we will discuss a methodology to incorporate CNSS standards in an applied manner through lab exercises, using the exercises to re-enforce concepts discussed in a more academic context. The paper is outlined as follows: in section II we provide background and introduce the CNSS standards, in section III we describe a masters level curriculum in IA. In section IV we propose lab examples that re-enforce the curriculum, in section V we discuss a mapping methodology to map

Ronald C Dodge JR, *United States Military Academy*,
Ronald.dodge@usma.edu
Helen Armstrong, *School of Information Systems, Curtin University of Technology*,
helen.armstrong@cbs.curtin.edu.au

ISBN 1-933510-96-7/\$15.00 © 2009 CISSE

lab objectives to the CNSS standards, and in VI we conclude.

II. BACKGROUND AND THE CNSS STANDARDS

Creating and maintaining programs to develop information assurance professionals is a critical step in securing our information infrastructure. Degree programs and certifications have been developed to meet this need. Government and industry have adopted minimum requirements in education and training for a variety of information security roles. To support this need the U.S. department of defense created the National Academic Centers of Excellence in Information Assurance (CAEIA). The goal of this program is to reduce vulnerability in our information infrastructure by promoting higher education and research in IA and producing professionals with IA expertise in various disciplines. Additionally within the U.S. Department of Defense, the Office of the Assistant Secretary of Defense for Networks and Information Integration (ASD (NII)) established the Department of Defense Information Assurance (IA) Scholarship Program (IASP) grant and scholarship competition. The program is designed to:

- increase the number of new work force entrants who possess key Information Assurance skill sets;
- build the nation’s IA infrastructure through grants to colleges and universities jointly designated by the National Security Agency (NSA) and Department of Homeland Defense as Centers of Academic Excellence in Information Assurance Education; and
- develop and retain well-educated personnel who support the Department’s critical IT management and infrastructure protection functions.

For purposes of the IASP program, Information Assurance encompasses the scientific, technical, and management activities that ensure computer and network security, such as:

- Systems/network administration and operation
- Systems security engineering
- Information assurance systems and product acquisition
- Cryptography
- Threat and vulnerability assessment (includes risk management)

- Web security
- Computer emergency response team operations
- Information assurance training, education and management
- Computer forensics
- Defensive information operations
- Critical information infrastructure assurance

These programs (joined in 2001 by the National Science Foundation’s Scholarship for Service program) together have served as the “starter fertilizer” for the IA career field. The CAEIA program provides an incentive program for universities and colleges to develop IA faculty and degrees. As a prerequisite evaluation criterion for the CAEIA, schools must demonstrate that the curriculum effectively addresses CNSS Training Standard 4011, and at least one additional CNSS Training Standard (4012, 4013, 4014, 4015, or 4016).

A. Committee on National Security Systems (CNSS)

The CNSS standards have been the foundation of the Center of Excellence in Information Assurance since the inception in 2000. These standards were established as the National Security Telecommunications and Information Security Systems Commission (NSTISSC) in 2000 in response to Presidential Decision Directive 63 (PDD 63) on critical infrastructure protection [2]. PDD 63 documented a shortage and need for more information assurance professionals and called for the establishment of national training standards in information assurance [3]. The NSTISSC was later renamed the Committee on National Security Systems (CNSS).

Of the sixteen CNSS instructions associated with information assurance, there are six standards used by the U.S. National Security Agency (NSA) and the Department of Homeland Security (DHS) to certify educational institutions as Centers of Excellence in Information Assurance Education. The criteria used to map curricula for certification in information assurance is shown in Table 1. Each standard targets a particular sector within the information assurance field.

Table 1: NSA/DHS National IA Education & Training Program Standards

Standard	Target
<i>NSTISSI-4011</i>	<i>National Training Standard for Information Systems Security (INFOSEC) Professionals</i>
<i>CNSSI-4012</i>	<i>National Information Assurance Training Standard for Senior Systems Managers</i>
<i>CNSSI-4013</i>	<i>National Information Assurance Training Standard For System</i>

	<i>Administrators (SA)</i>
<i>CNSSI-4014</i>	<i>Information Assurance Training Standard for Information Systems Security Officers</i>
<i>NSTISSI-4015</i>	<i>National Training Standard for Systems Certifiers</i>
<i>CNSSI-4016</i>	<i>National Information Assurance Training Standard For Risk Analysts</i>

B. Experiential Learning in IA

The effectiveness of hands-on exercises to enhance education and training is well documented over several disciplines [4, 5, 6, 7]. The specific benefits of experiential learning are well presented by Felder [8]. Kolb’s Experiential Learning Theory [9] also supports the effectiveness of this type of educational experience. This theory defines a four stage learning cycle accommodating students with different learning styles. These cycles include a concrete experience; observation and reflection; forming abstract concepts; and testing in new situations. Hoffman and Conklin [5, 6] describe the effectiveness of experiential programs in IA curriculum. Most IA lab exercises involve the use of computers, stand alone or connected to a network, to work through the process of IA administrative or security tasks. Beginning in 2001, virtualization has become a mainstay to increase the scalability and reduce the cost of hosting lab exercises [10].

The core exercises in education and training programs have little variation. In forensics programs, imaging a hard drive is a core competency. In training, the steps in the collection of evidence are very important. Tools are typically left to interpret the data and produce information. In education, the understanding of what information can be gleaned from the data is the most important result. Exercises in training tend to focus on the use of tools and interpretation of the results. In education, the labs use very rudimentary tools to require a more low-level understanding of the data and then re-enforce the concepts with the tools used in the training exercises. As an example, a forensics lab exercise supporting a training curriculum might use a well known open source or commercial tool (Helix, FTK, or Encase) to image a drive and conduct all of the analysis. In an educational lab, the exercise might require a student to actually write the program that reads the data from the media and present it for human use or further automated processing (requiring a more in-depth understanding of the FAT, NTFS, EXT3, HFS, ect.). The lab is then followed up with the assessment of the same media using a tool similar to those used in training. This combination of education and training tools provides students a more

complete understanding of the topic while at the same time providing practical experience in applied techniques.

As in the forensics example used above, almost all IA topics can be similarly decomposed into an application or training level understanding and a more low-level fundamental understanding.

III. MASTERS INFORMATION ASSURANCE CURRICULUM

Before describing how the CNSS training standards can be effectively included in higher educational curriculum, we first will describe common components¹ of a Certificate or Master's level IA curriculum to serve as a reference point. Course titles vary, however the topic areas can be categorized in the following areas:

- Operating Systems
- Networking
- Cryptography
- Forensics
- Incident Response
- Risk
- Cyber Law

Certainly many other topic areas can be included, for example secure programming or security management. However to manage the list we use the above list as a non-exclusive example of topics. The core areas described above should all have a foundation in the security triad; confidentiality, integrity, and availability balanced against functionality. The curriculum used by NOVA Southeastern University is [11]:

Core Courses:

- Operating Systems
- Database Systems
- Software Engineering
- Computer Networks
- Client-Server Computing
- Secure Computer Systems
- Applied Cryptography
- Database Security
- Advanced Network Security
- Information Security Project

Electives (selection of any two):

- Programming Languages
- Legal and Ethical Aspects of Computing
- Electronic Commerce on the Internet

¹ Reference programs include Norwich University, University of Tulsa, Carnegie Mellon Heinz College, NOVA Southeastern University, and the SEI Survivability and Information Assurance Curriculum foundation.

- Artificial Intelligence
- Decision Support Systems
- Human-Computer Interaction

The courses listed above cover the referenced topics in complete detail and serve as a good reference to use for a discussion of lab exercises. The mapping of a curriculum to the CNSS standards is not an exact science. The subjective analysis as to whether a topic is adequately addressed by the curriculum is one of the frequently challenged components of the CAEIA program. Well designed lab exercises addressing the learning objectives of the CNSS standards in addition to an institution's own objectives could provide a solid base for the development of IA curriculum.

IV. LAB EXAMPLES

Defining lab exercises for a curriculum is a continual process of updating as new operating systems, tools, and techniques are introduced. However, change can be managed and introduced only when a benefit is perceived. For example, a lab exercise to detect and identify malicious network traffic from network traces would not necessarily be impacted by the release of a new operating system. However a new vulnerability discovered in SSL might provide an opportunity to re-enforce a cryptography or network security topic.

The content of a lab exercise frequently will cross different topic areas and can be used to continually re-enforce or provide "foreshadowing" to future topics in addition to the target topic. To demonstrate this point, we will examine a botnet lab exercise. The objective of the exercise is to increase student understanding of the concept of botnets and the security measures associated with detecting and mitigating this threat. The depth of the exercise can vary from training (where the entire lab is executed in one lesson) to a more in-depth analysis (where each component might be the topic of a lesson). Upon completion of this lab experience, students should understand at the awareness level how botnets can be created and deployed and at a more in-depth level, understand the application of more detailed fundamental concepts like Operating Systems privilege separation.

This example details an environment to build and deploy a botnet. The exploit will start like many others; a user visits a compromised website and gets compromised. The bot will then not only allow control over the compromised computer, but it will also seek out other vulnerable systems and extend the size of the botnet. The lab exercise is configured to allow for exploration of malware signatures of a compromise on the target system as well from the network.

A. Lab Configuration

We can elect to use a variety of operating systems for the lab based on the tools selected. The specific lab described here uses a Windows XP virtual machine for the attack computer, a Linux based firewall/router, and Windows XP and 2003 virtual machines for the target computers. The configuration of the laboratory environment is shown in Figure 1.

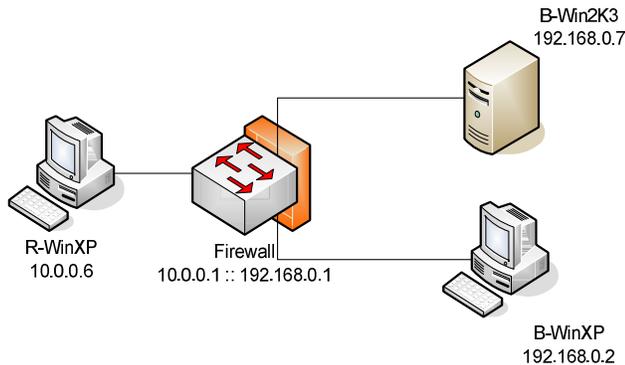


Figure 1 - Botnet lab virtual machine network

B. Lab Activity

The lab is broken down into four major phases as described below. The phases have been necessarily summarized and more information can be provided upon request.

1. **Setting up the attack computer:** The attack computer is set up in three stages. First, the development environment needs to be set up to compile the bot. For simplicity, we use lcc-win32 [12]. The student installs the executable (accepting all defaults). The next step is to configure the control channel using Office IRC. The student would install Office IRC and then launch the *Remote Control* application to configure a new IRC channel (call it “#botcontrol”). In the next step the student will mIRC (an IRC client) [13] to issue commands to your army of bots. The student will configure mIRC to connect to OfficeIRC on localhost and connect to the new control channel, “#botcontrol”.

For a more in-depth lab, the student can explore many additional technical facets including network protocols, how communication flows over the network, and firewall controls. The lab can also be used to discuss policy, security architecture, and trust.

2. **Compiling sdBot:** On the attack computer, start the lcc-win32 and open the sdBot C code file. The students will analyze the code to understand how it works and ensure the parameters are set to connect to the IRC server previously setup. After the code is compiled, a new file called “sdbot06b.err.exe” is created; this is the payload.

As with the first step of setting up the lab, there are many advanced concepts that can be discussed in this

phase, for example, this version of sdbot does not include any encryption. Inclusion of encryption or possibly assessing the impact of modifying the communication would address several more complex facets.

3. **Infecting the victim(s):** On the attack computer, the student verifies the file “bot.htm” is in the c:\inetpub\wwwroot directory and copies in the “sdbot06b.err.exe” file. On the target Windows XP virtual machine, the student opens an IE browser and navigates to the web site on the attack computer (http://10.0.0.6/bot.htm). On the victim Windows XP virtual machine, the student should run the *netstat* command and should then see an outbound connection to the IRC server and several connection requests on port 445 (this is the bot trying to spread!).

The third phase of this lab has components that cross all areas in information assurance; network and host level security controls are the most obvious advanced tasks that can be included.

4. **Wreaking havoc:** On the firewall, the student will start monitoring traffic flowing over the firewall using *Wireshark*. From the attack Windows XP virtual machine, the student will use mIRC to tell the bot to ping the firewall 100 times. This should see the pings on the *Wireshark* monitor on the firewall.

Phase 4 can be used in more advanced settings to evaluate defensive techniques and policies, for example students might develop IDS signatures to alert against the bot communicating over the command and control network.

C. Discussion

This lab provides a brief example of how you can, in an isolated and secure environment, create, configure, and experiment with malware. As described earlier, the full labs have much more detail and additional steps designed to explore techniques to prevent, discover, mitigate, and recover from exploitation. Additionally the labs can be expanded to assess the students' understanding of many additional advanced concepts. The focus of the lab is for the student to understand how malware gets on a target system, installed, and what it is capable of doing. In the context of the whole course, the intent behind using and understanding the malware is to understand how to detect, mitigate, and defeat it. Once the malware (whether it be a bot or another example) is understood, the student can follow additional labs that demonstrate the effectiveness of various defensive technologies. The concepts in the lab (whether the basic or advanced version) allow for reinforcement and assessment of many concepts that should be part of information assurance curriculum. The labs have another very compelling component that we propose: map the steps and objectives to the CNSS standards so that upon completion of a given lab exercise, a program can attest to the fact that the course maps to the selected CNSS standards. This mapping allows a

program to use the faculty lectures to explore more theoretical concepts and re-enforce/assess the topics in a more applied manner.

V. MAPPING METHODOLOGY

Course mapping to CNSS standards has always been a challenge for academic programs. The standards are difficult to map to a curriculum that is traditionally not tied to concrete examples. While the CNSS standards may be appropriate for and consistent with training standards, they cause some challenges for educational institutions that work towards an educational foundation for their students that will allow them to obtain higher levels of Bloom's taxonomy [14] of educational objectives. However, as described in section II, experiential based labs are shown to greatly enhance student comprehension. We offer that using the lab exercises to re-enforce a more academic focused curriculum has many benefits; from increasing student interest to assessing comprehension to mapping to CNSS standards.

In this discussion, we will focus our exploration of applying standards to lab exercises to CNSS-4011 (the standard that every program must map to). Within the standards there are three hierarchical levels: Function, Content and Topics. Each Function is presented in one of two levels of depth, Awareness and Performance. At the Awareness level the student creates a sensitivity to the threats and vulnerabilities of national security information systems, and a recognition of the need to protect data, information and the means of processing them; and builds a working knowledge of principles and practices in INFOSEC. Performance is defined as an understanding that provides the employee with the skill or ability to design, execute, or evaluate agency INFOSEC security procedures and practices. This level of understanding will ensure that employees are able to apply security concepts while performing their tasks. The Performance level has been used as the goal in the lab exercises referred to in this paper.

The seven Functions, categories, as well as a count of the associated Topics are enumerated in **Error! Reference source not found.2**. The Topic column lists only the number of Topics in the specified Content section. The total number of individual competency assessment Topics exceeds 230. This is minor compared to the Topics in CNSS-4013 - over 1320.

Table 2: CNSS-4011 Matrix

Level	Function	Content	Topics
Awareness	Communication basics	Historical background	1
Awareness	Communication basics	Technology Capabilities and Limitations	8

Level	Function	Content	Topics
Awareness	Automated Information Systems basics	Historical background	1
Awareness	Automated Information Systems basics	Hardware	4
Awareness	Automated Information Systems basics	Software	2
Awareness	Automated Information Systems basics	Memory	3
Awareness	Automated Information Systems basics	Media	2
Awareness	Automated Information Systems basics	Networks	7
Awareness	Security basics	INFOSEC overview	11
Awareness	Security basics	Operational Security	4
Awareness	Security basics	Information Security	3
Awareness	Security basics	INFOSEC	9
Awareness	NSTISS basics	National Policy and Guidance	4
Awareness	NSTISS basics	Threats to Vulnerabilities of Systems	3
Awareness	NSTISS basics	Legal Elements	4
Awareness	NSTISS basics	Countermeasures	6
Awareness	NSTISS basics	Concepts of Risk Management	5
Awareness	NSTISS basics	Concepts of System Life Cycle	6
Awareness	NSTISS basics	Concepts of Trust	3
Awareness	NSTISS basics	Modes of Operation	4
Awareness	NSTISS basics	Roles of Various Organizational Personnel	11
Awareness	NSTISS basics	Facets of NSTISS	13
Awareness	System Operating Environment	Automated Information Systems	3
Awareness	System Operating Environment	Telecommunication Systems	2
Awareness	System Operating Environment	Agency Specific Security Policies	3
Awareness	System Operating Environment	Agency Specific AIS and Telecommunications	2
Performance	NSTISS Planning and Management	Security Planning	4
Performance	NSTISS Planning and Management	Risk Management	6
Performance	NSTISS Planning and Management	Systems Life Cycle Management	6
Performance	NSTISS Planning and Management	Contingency Planning/Disaster Recovery	8
Performance	NSTISS Policies and Procedures	Physical Security Measures	13
Performance	NSTISS Policies and Procedures	Personnel Security Practices and Procedures	6
Performance	NSTISS Policies and Procedures	Software Security	13
Performance	NSTISS Policies and Procedures	Network Security	5
Performance	NSTISS Policies and Procedures	Concepts of Risk Management	13

Level	Function	Content	Topics
Performance	NSTISS Policies and Procedures	Auditing and Monitoring	9
Performance	NSTISS Policies and Procedures	Cryptosecurity	3
Performance	NSTISS Policies and Procedures	Key Management	5
Performance	NSTISS Policies and Procedures	Transmission Security	14
Performance	NSTISS Policies and Procedures	TEMPEST Security	8

The following step is to assess the lab exercise and determine which of the Topics applies. In this paper we only examine the topics in CNSS-4011, but in actuality the lab exercise would be assessed against all six standards and any mapping would be noted. As an example, we will assess only one of the Function/Content rows in Table 2; the NSTISS Policies and Procedures/INFOSEC Overview row. The complete Topic list is shown in Table 3.

Table 3: Security Basics/INFOSEC Topic Collection

Function	Content	Topic
Security basics	INFOSEC Overview	critical information characteristics - availability
Security basics	INFOSEC Overview	critical information characteristics - confidentiality
Security basics	INFOSEC Overview	critical information characteristics - integrity
Security basics	INFOSEC Overview	information states - processing
Security basics	INFOSEC Overview	information states - storage
Security basics	INFOSEC Overview	information states - transmission
Security basics	INFOSEC Overview	security countermeasures - Technology
Security basics	INFOSEC Overview	security countermeasures - education, training and awareness
Security basics	INFOSEC Overview	security countermeasures - policy, procedures, and practices
Security basics	INFOSEC Overview	security countermeasures - technology
Security basics	INFOSEC Overview	threats
Security basics	INFOSEC Overview	vulnerabilities

The botnet lab exercises described above can map to each of the Topics listed in Table 3. Lab exercises can either be developed from scratch to fulfill the requirements of each Topic or current lab exercises can be modified to ensure coverage of the Topic at the Awareness or Performance Levels.

The Topics can be mapped to existing lab exercises in two steps. The first links the Topics to the exercise through the tasks that must be carried out, and ensures the coverage of the Topic in the selected CNSS standard is complete. It is also advisable to map the exercise tasks to additional Topics in the same standards in addition to the other CNSS standards. The second step is to include

specific knowledge assessment questions that the student must answer at various points in the lab to confirm the desired learning has taken place.

As an example, for the Topic “critical information characteristics – confidentiality” the task could be to either modify the bot to exchange data with the command and control node using encryption to develop a technical control where sensitive data on a system would be protected in the event a bot was introduced to the machine. Additionally, the student could be asked to describe data storage policies required to protect local data from exposure. This particular lab exercise would then map to more than one Topic. In this instance the additional topics of Security Countermeasures – Technology, and Security Countermeasures – Policy, Procedures and Practices could be included in the mapping.

Previous work by Dodge, Hay and Nance [15] and Armstrong [16] indicates that many of the Topics overlap across the six CNSS standards. This provides an advantage to those institutions attempting to gain the CAEIA NSA accreditation.

VI. CONCLUSION AND FUTURE WORK

In order to gain CAEIA certification from the NSA, schools must demonstrate that the curriculum effectively addresses CNSS Training Standard 4011, plus one additional CNSS Training Standard from the 4012, 4013, 4014, 4015, or 4016 set. The work involved in submitting for CAEIA is substantial, however, such accreditation provides recognition that a baseline of IA topics

As tertiary education institutions move toward greater recognition from national and international standards bodies, the use of lab exercises can aid the CNSS accreditation process. Although the mapping of IA lab exercises to these standards is not a straight forward task, the overlapping nature of the standards means that a single lab exercise can be readily modified to meet the requirements of more than one Topic in a single standard, in addition to fulfilling requirements in similar Topics in other standards.

The development of a repository of lab exercises specifically designed and modified to meet the CNSS standards is a reachable goal for the near future. If such a repository were freely available, this would allow institutions to choose those exercises that provided a best fit to their own institution’s objectives and at the same time ensure compliance with the CNSS standards.

VII. REFERENCES

- [1] Spafford, G, "Centers of Academic Adequacy", http://www.cerias.purdue.edu/site/blog/post/centers_of_academic_adequacy/, last accessed 9 March 2009
- [2] NSA, IACE – Courseware Evaluation Program, <http://www.nsa.gov/ia/academia/iace.cfm>
- [3] White House, PDD 63, Critical Infrastructure Protection, <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>,1998 Last accessed on 2 March 2009.
- [4] Hoffman, L.J.; Rosenberg, T.; Dodge, R.; Ragsdale, D., Exploring a national cybersecurity exercise for universities, Security & Privacy, IEEE, Volume 3, Issue 5, Sept.-Oct. 2005 Page(s):27 – 33
- [5] Conklin, A, Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course; 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference, Volume 9, 04-07 Jan. 2006 Page(s):220b – 220b
- [6] Greenberg, J.E.; Delgutte, B.; Gray, M.L. Hands-on learning in biomedical signal processing, Engineering in Medicine and Biology Magazine, IEEE, Volume 22, Issue 4, July-Aug. 2003 Page(s):71 – 79
- [7] Mountain, J.R, Work in progress – applied process control systems design: hands-on laboratory experiences for multiple disciplines and academic levels, Frontiers in Education, 2004. FIE 2004. 34th Annual, 2004 Page(s):T1D – 3-4 Vol. 1
- [8] Felder, R.M., Reaching the Second Tie—Learning and Teaching Styles in College Science Education, J. College Science Teaching, vol. 23, 1993, pp. 286–290.
- [9] D..A. Kolb, Experiential Learning: Experience as the Source of Learning and Development. Prentice-Hall, Inc., Englewood Cliffs, N.J. 1984.
- [10] Schafer, J., Ragsdale, D., Surdu J., Carver, C., The IWAR range: a laboratory for undergraduate information assurance education, Proceedings of the sixth annual CCSC northeastern conference on The journal of computing in small colleges, p.223-232, April 2001, Middlebury, Vermont, United States
- [11] NOVA Southeastern University IA Masters Curriculum, http://infosec.nova.edu/ms_info_sec.html, last accessed on 2 March 2009.
- [12] lcc-win32 retrieved on December 18, 2007 from <http://www.cs.virginia.edu/~lcc-win32/>
- [13] mIRC retrieved on December 18, 2007 from <http://www.mirc.com/>
- [14] Bloom, B. S. Taxonomy of educational objectives: Handbook I: Cognitive domain. Longmans, Green & Company, 1956
- [15] Dodge, R., Hay, B., Nance, K., Standards-based cyber exercises, Proceedings of Organizational Security Aspects (OSA) 2009, 16-19 March, Sukuoka, Japan
- [16] Armstrong, H., 2007, Mapping information security curricula to professional accreditation standards, Proceedings of the 2007 IEEE Information Assurance Workshop, pages 30-38, West Point, NY, 20-22 June 2007