2007

Experiences and lessons learned in the design and implementation of an Information Assurance curriculum

Sreekanth Malladi
Dakota State University

Omar F. El-Gayar
Dakota State University

Kevin Streff
Dakota State University

Experiences and lessons learned in the design and implementation of an Information Assurance curriculum

Conference Paper · July 2007

DOI: 10.1109/IAW.2007.381909 · Source: IEEE Xplore

3 authors, including:

Omar F. El-Gayar
Dakota State University
156 PUBLICATIONS **1,501** CITATIONS

SEE PROFILE

Kevin Streff
Dakota State University
24 PUBLICATIONS **178** CITATIONS

SEE PROFILE

Proceedings of the 2007 IEEE
Workshop on Information Assurance
United States Military Academy, West Point, NY, 20-22 June 2007

Experiences and lessons learned in the design and implementation of an Information Assurance curriculum

Sreekanth Malladi, Omar El-Gayar, Kevin Streff

Abstract—
In 2004, Dakota State University proposed a model for information assurance and computer security program development. That model provided a framework for developing undergraduate and graduate programs at DSU. This paper provides insight into experiences and lessons learned to further implement that model. The paper details modifications to both the undergraduate and graduate information assurance programs as a result of specific issues and challenges. Further, the paper highlights the introduction of a new terminal degree that includes an information assurance specialization. As a national center of excellence in information assurance education, we are confident that this paper will be helpful to universities around the world in either developing new or improving existing IA programs.

Keywords—**IA curriculum, IA education, Graduate programs, IA discipline.**

I. Introduction

Dakota State University has been ranked No. 1 among U.S. Midwest public universities and colleges by U.S. News and World Report in 2006 and is a national center of excellence in information assurance education. We have implemented a Bachelors in Computer and Network Security (CONS) in 2002 and a Masters in Information Assurance (MSIA) in 2004. We also offer a minor in Computer and Network Security and a newly proposed minor in Digital Forensics.

Recently the faculty analyzed both the graduate and undergraduate information assurance programs, keeping in mind the latest trends and requirements of the IA discipline (both industry and academic), learning from our past experience in implementing the IA curricula, and looking into the future to expand IA with our recently introduced D.Sc. program. In this paper we detail the issues and challenges with the IA program, highlight lessons learned over the past several years, and outline the revised IA program to help other universities interested in introducing or improving their information assurance program.

II. Literature review - IA education

Information assurance (IA) is defined as
"Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" [1].

Information assurance education involves efforts to educate a workforce with the needed knowledge and skills to assure our information systems and critical infrastructures. Information assurance education continues to grow in importance as IA programs develop across the country. A brief look at information assurance education history offers insight into this evolution.

The National Information Assurance Education and Training Partnership (NIETP) program is a collaboration among industry, government, and academia centered on advancing information assurance education, training, and awareness. The NIETP was started in 1990 under National Security Directive 42, serves as a national manager for information assurance education and training related to national security systems, and coordinates this effort with the Committee on National Security Systems (CNSS). CNSS is responsible for the development of principles, policies, guidelines, and standards that concern systems related to national security information. Education and training standards are among the many standards and guidelines that CNSS issues [1].

Academia is involved in NIETP activities through the National Centers of Academic Excellence in Information Assurance Education (CAEIAE) Program. The CAEIAE program was started in 1998 by the National Security Agency (NSA) and is now jointly sponsored by the NSA and the Department of Homeland Security (DHS) in support of the President's National Strategy to Secure Cyberspace. The purpose of the program is to recognize and support academia for their efforts in information assurance education and to facilitate further development of these programs in information assurance. In 2006, there were 75 institutions designated as CAEIAE schools [2]. Schweitzer et al. present the ten criteria to become a CAEIAE and how to go about a successful application [3].

In 2001, the ACM and the IEEE-CS published Computing Curricula 2001 which contains curriculum recommendations for undergraduate programs in computer science. That report also called for additional discipline-specific volumes for each of computer engineering, information systems, and software engineering [4]. IT2005 and CC2005 are additional IT curriculum standards that are based on the Information Technology Body of Knowledge. Information Assurance and Security (IAS) is one of a dozen domains within this body of knowledge and includes 23 core teaching hours within the 281 hour standard. Dark et al. described the Information Assurance and Security (IAS) component of the IT2005 document [5]. At the 9th annual Colloquium for Information System Security Education in Atlanta, GA, re-

College of Business and Information Systems, Dakota State University.

ISBN 9-9999-9999-9/99/ $20.00

searchers introduced CC2005 and IT2005 to the IA education community [6]. Kamali et al. described using the curriculum model developed by the SIGITE Curriculum Committee [7].

Finally, several articles have been published to help educators develop and hone their information assurance and computer security programs. Dennis et al. further outlined a model information assurance and computer security program [8] (See Figure 1). Streff et al. described the educational components of Dakota State University's nationally-recognized information assurance program and provided an overall description of the program, including how it evolved from no security class to a comprehensive undergraduate computer and network security program [9].

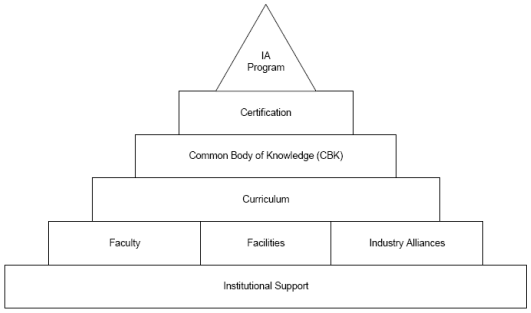

Fig. 1. A model for IA and computer security program development [8]

III. Programs' background

The IA undergraduate curriculum started with a Bachelor of Science in E-Commerce and Computer Security major in 2000. This seminal program did not include dedicated security courses. The program was revamped in 2002 with the introduction of the first such course, *Computer Security Fundamentals*. The program was extended in 2003 with four additional security courses: *Cyber Law, Network Security, Intrusion Control and Detection* and *Cryptography/Info Assurance*. This program evolved into the Computer and Network Security (CONS) major in 2005 with the addition of two more security courses - *Systems Programming* and *Computer Forensics*. Nine incoming freshmen elected the CONS major in 2005 and the number increased to 20 in 2006.

The Master of Science in Information Assurance (MSIA) was started in Fall 2004. The program addressed a distinct need for comprehensive information assurance programs at the regional and the national levels. The program also sought to capitalize on the universities recent designation by the National Security Agency as a Center of Academic Excellence (CAE). Consisting of 36 credits of IA coursework, including eight core courses and three specialization courses in *Wireless/Mobile Security, Banking/Financial Security,* or *Cyber security*, the program is designed to prepare professionals with the skills to develop and implement security strategies and to provide technical leadership so as to improve the security posture of organizations. In Fall 04, the program started with 20 applications resulting in 16 students actually enrolled in the program. The majority of this group was students graduating with a B.S. in CONS from DSU. The following two years the program seemed to have stabilized at 12 students enrolling in the program. A number of the students who entered the program in Fall 2004 have already successfully completed all program requirements and have graduated from the program. These alumni have been successful in finding full-time jobs in the region.

Another graduate level program at DSU, the Master of Science in Information Systems, also has a specialization in Network Administration and Security. This specialization included a course called *Network Security and Intrusion Detection* (INFS 754) well before the MSIA was started. This course is shared with the MSIA curriculum

IV. Issues and Challenges in implementing the IA curriculum

A number of issues and challenges have emerged over the course of implementing the undergraduate and graduate IA programs. While some issues were specific to a particular program, others were pervasive through undergraduate and graduate programs. The following sections detail some of these issues.

A. Student backgrounds

Universities typically have students with varying backgrounds and academic preparation. Accordingly, it is important for any major to properly consider this and tune the curriculum to fit the backgrounds of the students. At Dakota State University the undergraduate CONS students have little interest in mathematical or computer programming concepts. However, it was felt that this was largely due to the curriculum itself not training students with those concepts early in their college experience. At the graduate level, students are required to have an undergraduate degree in computer science, information systems, or an information technology related field. With the exception of computer science undergraduate, it was evident the students do not have adequate mathematical foundation to prepare for advanced graduate courses such as cryptography. Moreover, while students enter the program with programming skill, their knowledge of system level programming does not meet the requirements for some of the technical courses in the curriculum such as *Software security, Network security*, and *Computer forensics*.

B. Lab infrastructure

Huss explains that the outcome of a well-structured lab experience will "solidify and expand student knowledge about various aspects of computer security" [10]. Mattord et al. outlined how to plan, build and operate an information security and assurance lab [11]. Tikekar et al. outlined the specific challenges in designing information assurance lab exercises [12]. DSU has certainly encountered many of these issues. In particular, it was noticed that the IA lab activity is complicated mainly because of the following issues:

1. The risk of interference with normal university activity,

2. Ability to handle the lab exercises without expert guidance (a problem distance students often face),
3. Legal and ethical issues.

C. Graduate programs specific issue

The MSIA program originated as a traditional graduate program where students will have to attend courses on campus preferably as full-time students working their way through the program in cohorts. However, as the program matured, inquiries by prospective revealed the following:

- Information systems and computer security professionals wishing to advance their careers and specialize in information assurance, wish to do so while keeping their current jobs.
- Likewise, computer science and information systems students are interested in pursuing the program in conjunction with starting their first job.

In either case, it became evident that the opportunity cost for prospective students (with their specialized technical background) is simply too high to afford a full-time resident program. Despite DSU's infrastructure and experience delivering online graduate programs ([13], [14]), a unique challenge facing the online delivery of the MSIA program is meeting the requirements for technical courses.

Moreover, the original program structure required student to complete the program in cohorts. While this model has had some success in other programs, it became apparent that the cohort structure is too restrictive to address the needs of computer security professional. To accommodate flexible student plans of study, it became necessary to revisit and explicate the prerequisites of the individual courses as will be described later in the paper.

D. Undergraduate programs specific issues

Several issues were evident in our undergraduate program:

1. The program was heavily focused on network security and lacked an emphasis on software security. While software security was infused in many of these network security courses, the program lacked focus on the issues and solutions surrounding designing, building and testing software.
2. Students lacked the prerequisite programming knowledge to study advanced network and software security concepts. Students were taking two semesters of Visual Basic .NET, which did not prepare them for the significant programming required for our network security courses and the software security courses on the drawing table.
3. The program did not adequately address managerial topics - while our MSIA program has several classes dedicated to managerial security concepts (i.e., risk assessment, policy and procedures, business continuity planning, etc.), our undergraduate program is lite on these topics. While the program needs to have a heavy technical orientation, it could use better balance with managerial components.
4. The students lacked a fundamental understanding of information assurance before their senior year. The first real security course was taken during the student's senior year. Students took technology courses before then; however, they did not get the big picture or any security prior to their senior year. This was de-motivating to security students and also did not provide them an early indicator if they really liked the major.

The program was becoming very popular with undergraduate students; however, the faculty felt that the program needed to evolve to address these issues early on.

V. Changes to the IA programs

In the previous section the issues and challenges in the IA curriculum were discussed. In this section the changes to the old curriculum will be presented along with the new curriculum that evolved as a result of these changes. First the undergraduate curriculum is covered and then the graduate curriculum.

A. Undergraduate curriculum changes

DSU offers a B.S. in Computer and Network Security, as well as two minors that augment the B.S. in Computer Science and B.S. in Computer Information Systems majors. Each is described further.

A.1 Bachelor of Science in Computer and Network Security (CONS)

Whitman et al. identified three general types of information assurance programs: technical, managerial, and balanced [11]. DSU's program has evolved from a technical program to a balanced program. Figure 3 describes the newly proposed curriculums. Figure 2 describes the structure and ordering of courses in the new design.

The new design has evolved recently with heavy internal discussions among the faculty through collecting past experiences, recent advances and trends in this field and the backgrounds of the student community. The new program includes a heavy technical emphasis and a better sequencing of courses to maximize student programming opportunities.

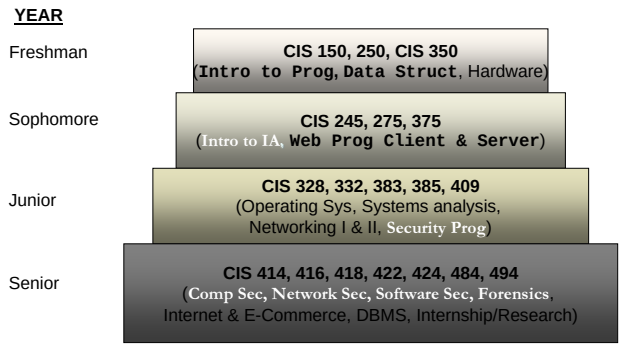

Fig. 2. Structure of the newly designed B.S in CONS major

The major changes in the curriculum and the factors that influenced the changes are described below:

1. **Inclusion of the new Introduction to Information Security & Assurance course.** Consistent with the recommendations of Bhagyavati et al. [15], DSU has integrated information security concepts throughout it's computer science and computer information systems programs. In addition, Whitman et al. identified that undergraduate information assurance programs should include an *Introduction to Information Security and Assurance course* [11]. This foundation course is typically lecture/discussion and surveys the breadth of information assurance topics, including understanding the key issues, developing protection and response strategies, and designing efficient detection and security systems. DSU has added CIS 245: *Principles in Information Security* course consistent with what Whitman and Mattord recommended in 2004. This course is intended to present a broad perspective of IA concepts to a general audience in a simple yet interesting way. The main goals of the course are to:

(a) Introduce IA concepts to the CONS majors early in their college education and,

(b) Expose IA concepts to all the majors thereby guaranteeing that every student has a decent knowledge of security.

Grimaila et al. presented their experience in the design, implementation, and teaching of a foundation undergraduate business information security course with laboratory components using security tools [16]. Dakota State has leveraged these experiences to include interdisciplinary teaching into its CIS 245 course.

2. **Changing the focus to programming and software oriented.** The most significant change of our undergraduate curriculum was changing the focus of the discipline into a strongly programming-based curriculum. Contrastingly, in our old curriculum we had little programming component with the students required to take only a basic programming course (CSC 150) followed by a web application programming (client-side) course. The temporal arrangement of these courses was also in a way, non-beneficial to the curriculum because those courses were often taken by students after they finished the IA core. Thus, the knowledge of programming they developed was of little use. In the present B.S. (CONS) curriculum, students develop a strong programming base before they start their IA core. They are required to take a *Data Structures* course, a *Web Application Programming* course (server-side) in addition to the existing ones. They also take a special programming course CSC 409 (titled *Systems and Security Programming*) before their core which enhances their programming for IA related concepts.

3. **Changing the focus of the IA core from network security centric to a proportionate mix of networking and software security.** The IA core has also undergone a significant change. Out of the four core courses, CIS 422: *Cryptography* has been removed and *Software Security* has been introduced. Spaford has communicated specific goals for Science and Technology programs, including teaching basic skills with an emphasis on a professional path [17]. DSU has aligned its program with professional paths, including information security management, network security, and software security jobs. Reynolds published regarding designing information technology curriculum with "pervasive themes" [18]. Prior to the aforementioned curriculum changes, Dakota State's undergraduate information security program was predominately a network security program. With these changes, the program has added a couple of pervasive themes: information security management and software security. As a result of being very network security centric, the DSU undergraduate information assurance program included almost 200 hours of cryptography content. Al-Hamdani et al. suggest that approximately 100 hours of cryptography is sufficient in an undergraduate security program [19]. Therefore, DSU revised the curriculum to include 100 hours of cryptography content and used these "freed up" 100 hours for information security management and software security content. Researchers concluded that security course content and structure are appropriate for the skill set needed for various security jobs. However, the researchers determined that neither the present course structure nor the security jobs will be able to mitigate the root causes of the security vulnerabilities as academia and industry are going after symptoms, and not after the cause of the symptoms: Incorrect software. Consistent with the findings of Pothamsetty [20], Dakota State enhanced its emphasis on software security by adding a software testing class and integrating information security in the system analysis and design class. Dreher indicated that technology programs should consider a course focused on hardware and software systems security [21]. With a strong exposure to networking, followed by *Computer Security Fundamentals* and *Software Security*, the students enter CIS 416: *Network Security*. This well structured manner offers more leverage to the instructor for CIS 416 to include advance concepts in network security which is the true culmination of most of the technical aspects of security.

4. **Inclusion of IA related concepts and courses as part of every major.** Bogolea et al. presented a case study on an approach to creating an undergraduate curriculum that augmented existing degree programs in Computer Science and Information Technology [22]. Wilkens et al. identified ten emerging areas in computer science, including computer and network security, information assurance, robotics, bio-informatics, animation, game programming, web application development, embedded computing, wireless computing, and grid computing [23]. DSU has involved computer science majors in the IA program in a couple of ways. First, computer science students are encouraged to minor in computer and network security. Second, many of the computer science classes include IA modules. Finally, several computer science students have matriculated to the MSIA program.

Little doubt remains regarding the need to update undergraduate computer science curriculum to teach information assurance and security concepts. Many models exist. One model is to develop an undergraduate track in computer security [24]. Another approach is to infuse information security concepts throughout the existing computer science curriculum. DSU has utilized both

approaches to ensure computer science, computer information systems and computer and network security majors all receive information security knowledge in their programs.

Pref	Num	Title	Cr Hrs
General Education			41
Required courses			54
CIS	**245**	**Info Sec Fund**	**3**
CIS	275	Web Programming I	3
CIS	328	Operating Env	3
CIS	332	Systems Analysis	3
CIS	350	Comp HW, Data, Net	3
CIS	375	Web Programming II	3
CIS	383	Networking I	3
CIS	385	Networking II	3
CIS	388	Comp Forensic Fund	3
CIS	414	Computer Security	3
CIS	416	Network Security	3
CIS	418	**Adv Forensics**	3
CIS	422	**Software Security**	3
CIS	424	Internet & E-Comm	3
CIS	484	Database	3
CIS	494	Internship	3
	or	Operating Systems	
CIS	498	Undergrad Research	
CSC	250	Computer Science II	3
CSC	409	System & Sec Prog	3
Required support courses			18
Bad	336	Entrep I	3
Bad	406	Acct for Entrep	3
Bad		Elective course	3
Engl	208	Doc & Pres	3
Mat	201	Intro to Applied Math	3
Mat	281	Intro to Statistics	3
	or		
Bad	220	Business Statistics	
Electives			15
Total number of hours required			**128**

Fig. 3. The new B.S in CONS curriculum

A.2 Digital forensics minor

Cooper explored the concept as applied to Digital Forensics as a distinct academic discipline from other computing sciences [25]. At the curriculum level, Champlain College for undergraduate education (`http://digitalforensics.champlain.edu/`) and Sam Houston State University for graduate-level education (`http://www.df.shsu.edu`) are early pioneers in forensics education. Consistent with the thinking of Cooper, Dakota State has made a significant development in our undergraduate curriculum has been the inclusion of a minor in Digital Forensics. This was possible largely with the development of relevant faculty expertise through training and certification. The required support courses to obtain a minor in Digital Forensics are listed in Figure 4.

Prefix	Number	Course Title	New*	Hours
CIS	245	Information Security Fund.		3
CIS	385	Networking II		3
CIS	388	Computer Forensic Fundamentals		3
CIS	414	Computer Security		3
CIS	418	Adv Computer Forensics		3
CIS	4xx	Defense & Forensic Counter-measures	x	3
CIS	4xx	Computer Forensics & Investigations	x	3
		Subtotal, required		21

* New: Y= yes, N = no.

Fig. 4. B.S with Digital forensics minor

Researchers from the Rochester Institute of Technology concluded that undergraduate forensic courses should be designed to provide students with the ability to identify and employ tools used for tracking intruders, gathering, preserving and analyzing evidence of their activities. They also indicated that courses must emphasize both the fundamental computer forensics techniques and the hands-on experience of utilizing the tools needed to uncover illegal activities of computer users. Dakota State has integrated forensics techniques and hands-on tools into the minor in digital forensics to ensure a quality student learning experience.

A.3 Computer and Network Security Minor

DSU has many students studying Computer Information Systems (CIS) and Computer Science (CS). Dakota State has integrated these students into the field of information assurance in a couple of ways. First, many of the CIS/CS classes include IA modules. Second, several CIS/CS students have matriculated to the MSIA program. Finally, CIS/CS students are encouraged to minor in computer and network security. Figure 5 outlines the minor in computer and network security.

Pref	Num	Title	Cr Hrs
CIS	**245**	**Info Sec Fund**	**3**
CIS	350	Comp HW, Data, Net	3
CIS	383	Networking I	3
CIS	385	Networking II	3
CIS	414	Computer Security	3
CIS	416	Network Security	3
Total number of hours required			**18**

Fig. 5. B.S with CONS minor

As of March, 2006 DSU has 74 students who are electing this minor.

B. Graduate curriculum changes

This section covers the changes in the curriculum at the graduate level. The MSIA program is first introduced followed by the newly developed Doctor of Science (D.Sc.) program with an IA specialization.

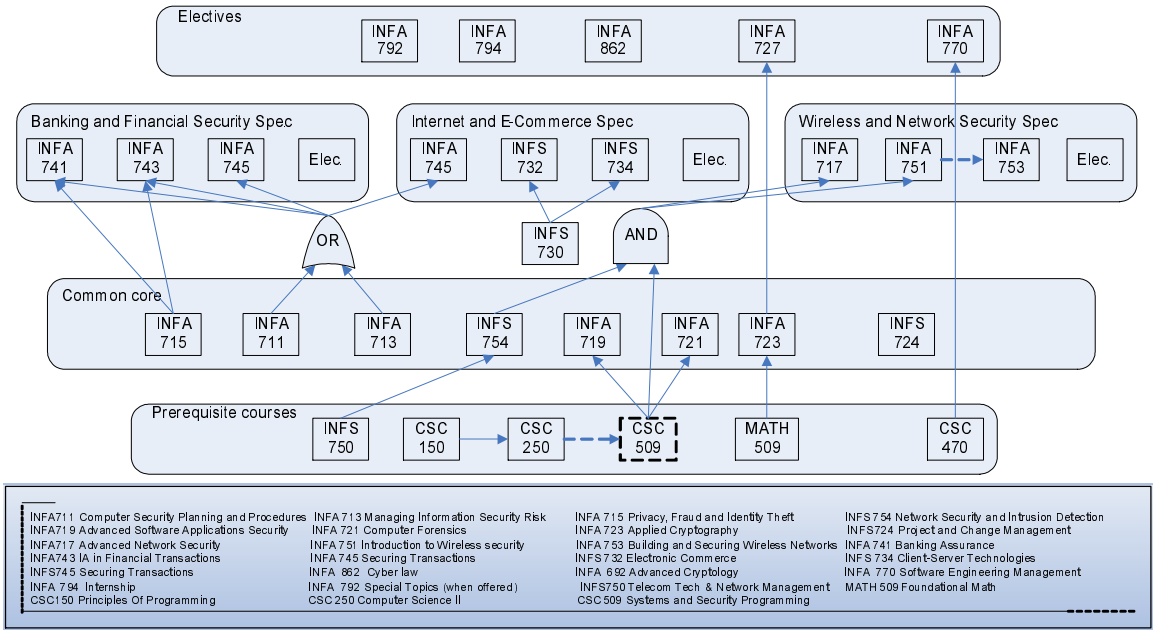

Fig. 6. MSIA course structuring

B.1 Master of Science in Information Assurance

Figure 6 describes the general ideology behind the MSIA program. The main changes to the Master's program were aimed at addressing student background, accommodating distance delivery, and eliminating the cohort system. To ensure adequate preparation of students entering the program, students are required to take two knowledge support courses before they start the relevant core IA courses, in particular, *Applied Cryptography* and *Software Security*. These courses are Math 509 - *Foundations of Math* and CSC 509 - *Systems and Security Programming*. Experience from teaching the above courses suggested that they added valuable knowledge to the students that enabled them to better understand and handle the subsequent core courses. The mathematical concepts in Math 509 were fine tuned to be more befitting the needs of Cryptography and CSC 509 for Software Security (low-level C/C++ combined with some assembly is the focus of this course).

Accommodating distance delivery involved analyzing the content and the requirements of the individual courses in the MSIA core and redesigning the courses to be better suited for distance delivery. The changes include:

- Emphasizing the use of open source tools and utilities.
- Revising lab assignments so as students can complete these assignments by remotely accessing computing resources in the IA lab.
- Updating the IA lab infrastructure to allow for remote access of computing resources.

B.2 Towards a doctoral degree with an IA specialization

In December 2005, DSU received the South Dakota Board of Regents's approval to deliver its first doctorate degree. Capitalizing on its strengths in information technology in general and information systems in particular, the newly approved doctorate of science in information systems emphasizes applied scholarship, focusing on multi-disciplinary research projects with a strong emphasis on the productive application of information systems and information technology to organizations and their management. The degree requires a total of 88 credit hours including 27 master-level preparation. The program accommodates distance delivery and builds on the Master of Science in Information Systems (MSIS) program (including the Network Administration and Security specialization). The curriculum supports the following specializations: Decision support, knowledge and data management, information assurance, and information systems in health care. Included in the doctoral requirements are 9 credits of research methods, 6 credits of research seminars, 9 credits of specialization requirements, 12 credits of specialization electives, and 25 credits of dissertation. The information assurance specialization builds of two MSIA core courses (INFA 711 and INFA 713) with the addition of a doctoral level research course and up to 4 elective courses. Students opting for this specialization may address managerial, organizational, social, or technical topic pertaining to information assurance and computer security. Students may also leverage synergies inherent among the D.Sc. program. For example, students may elect to address privacy and security issues in the health care industry. Alternatively, students may develop decision support and knowledge management techniques to develop better

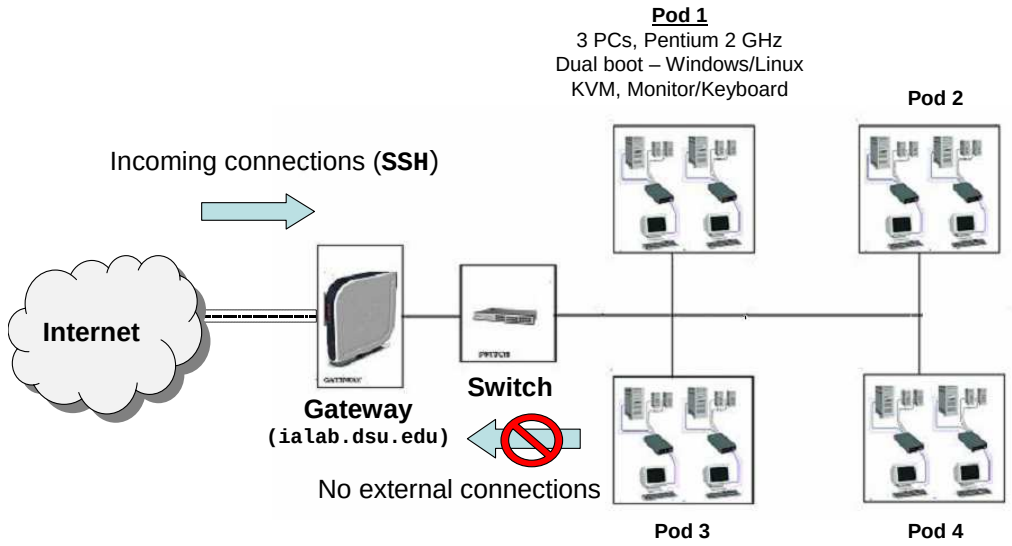

Fig. 7. Information Assurance Laboratory (IA Lab)

security tools and management models.

C. Changes to the lab and supporting infrastructure

To address the risk of interfering with normal university computing (e.g. through ARP poisoning) , a dedicated lab called the "IA Lab" (Figure 7) was created for students that is segregated from the university network (i.e. no outside connectivity from inside). Students are allowed to perform any kind of activity within the IA lab. The lab consists of machines with a variety of platforms and tools. Live CD distributions (e.g. Knoppix) that are loaded with several security tool collections are also used in the lab and were found to be quite useful. Lab sessions are now scheduled for students to handle the malicious lab activity. Benign activity (such as pinging, sniffing, and firewalling) is included in the home work assignments (these tools are covered in detail in the class). At the undergraduate level,

The IA Lab has also a special feature that enables inside access from outside (but not vice-versa). A special machine is included that acts as a gateway to the internal network. Students can first ssh to this machine from anywhere outside and subsequently ssh to one of the internal IA lab machines. Students can then perform exercises on the internal machines such as port-scanning other machines, sniffing and analyzing for vulnerabilities.

The external machine in the IA Lab is used to install servers that are to be accessible from outside for class use (such as a PGP key server). VMWare (Virtual Machine ware) is installed on all the machines in the lab. Windows Network Administration is a common activity that we require students to perform on VMWare images that can be discarded after the lab activity with no change to the real underlying OS.

Perhaps the most serious issues faced by the IA lab activity are the legal and ethical aspects of it. To address this, a significant change in the perspective of the IA program was made at all levels. It is explicitly stated in all the course syllabi and at other appropriate places that the IA programs or courses do not teach or train students to hack other computers or attack networks. Students do get exposure to hacking techniques only to gain a better understanding of how to defend against them. Indeed, before they learn how to defend against an attack, it is essential to know how attacks work. Accordingly, the curriculum, course contents and terminology was changed to reflect this policy:
DSU's IA programs provide training in IA and Security but not towards malicious activity resulting in criminal acts.

Wagner et al. published on the ultimate hands-one lab exercise: a cyber war competition [26]. DSU has utilized this approach by hosting a "Treasure Hunt" where students formed teams and captured network "flags". Each team defended its network while looking to penetrate other team subnets to find the hidden flags.

VI. Conclusion

This paper revisits the IA programs based on the model proposed by Dennis et al. [8] with an eye to implementation challenges and lessons learned for other IA academics. The paper summarizes the top implementation challenges to be the diverse student backgrounds, inadequate student programming knowledge, designing meaningful hands-on lab exercises for the students, legal and ethical issues with IA labs, and the distance delivery issues associated with IA programs. Further research includes assessing the viability of remote connection to the IA labs, including moving to a fully distance-enabled program. Ad-

ditional research in assessing the retention and success rates of students with diverse backgrounds is also necessary as well as following up with alumni and employer surveys.

REFERENCES

[1] CNSS, "Committee on National Security Standards," *National Information Assurance Glossary*, `http://www.cnss.gov/history.html`, June 2006.

[2] NSA, "National Security Agency," `http://www.cnss.gov/history.html`, 2007.

[3] D. Schweitzer, J. Humphries, and L. Baird, "Meeting the criteria for a center of academic excellence (cae) in information assurance education," *Journal of Computing Sciences in Colleges, Consortium for Computing Sciences in College*, vol. 22, october 2006.

[4] R. Shackelford, L. Cassel, J. Cross, J. Impagliazzo, E. Lawson, R. LeBlanc, A. McGettrick, R. Sloan, and H. Topi *35th SIGCSE technical symposium on Computer science education SIGCSE '04*, vol. 36, march 2004.

[5] M. Dark, J. Ekstrom, and B. Lunt, "Curriculum models: Integration of information assurance and security into the it2005 model curriculum," *Proceedings of the 6th conference on Information technology education SIGITE '05*, October 2005.

[6] J. Ekstrom and B. Lunt, "Integration of information assurance and security into it2005," *9th Colloquium for Information Systems Security Education*, june 2005.

[7] R. Kamali, S. Liles, C. Winer, K. Jiang, and B. Nicolai, "Curriculum models: An implementation of the sigite model curriculum," *Proceedings of the 6th conference on Information technology education SIGITE '05*, October 2005.

[8] T. Dennis, O. F. El-Gayar, and K. Streff, "A model program in information assurance and computer security," *IACIS International Association for Computer Information Systems 2004*, vol. 4, no. 2, pp. 97–102, 2004.

[9] K. Streff and Z. Zhou, "Developing and enhancing a computer and network security curriculum," *Consortium for Computing Sciences in Colleges. Journal of Computing Sciences in Colleges*, vol. 21, february 2006.

[10] J. Huss, "Laboratory projects for promoting hands-on learning in a computer security course," *ACM SIGCSE Bulletin*, june 1995.

[11] M. Whitman and H. Mattord, "Academic papers: Designing and teaching information security curriculum," *Proceedings of the 1st annual conference on Information security curriculum development InfoSecCD '04,*, october 2004.

[12] R. Tikekar and T. Bacon, "The challenges of designing lab exercises for a curriculum in computer security," *Consortium for Computing Sciences in Colleges, Journal of Computing Sciences in Colleges*, vol. 18, may 2003.

[13] T. Dennis, O. El-Gayar, and Z. Zhou, "A conceptual framework for hybrid distance delivery for information system programs," *Issues in Information Systems (IIS)*, vol. 3(1-2), 2002.

[14] O. El-Gayar and T. Dennis, "Effectiveness of hybrid learning environments," *Issues in Information Systems (IIS)*, vol. 6(1-2), 2005.

[15] S. Bhagyavati, M. Olan, D. Naugler, and C. Frank, "Tutorials, workshops and panels: Information assurance in the undergraduate curriculum," *Proceedings of the 43rd annual southeast regional conference*, vol. 1, March 2005.

[16] M. Grimaila and I. Kim, "An undergraduate business information security course and laboratory," *Journal of Information Systems Education*, vol. 13, 2002.

[17] E. Spaford, "Teaching the big picture of infosec," *National Colloquium For Information Systems Security Education (NCISSE), VA*, 1998.

[18] C. Reynolds, "IT education – curriculum development: Engineering the information technology curriculum with pervasive themes ," *Proceedings of the 7th conference on Information technology education SIGITE '06*, october 2006.

[19] W. Al-Hamdani and I. Griskell, "Pedagogy: A proposed curriculum of cryptography courses," *Proceedings of the 2nd annual conference on Information security curriculum development InfoSecCD 05*, september 2005.

[20] V. Pothamsetty, "Pedagogy: Where security education is lacking," *Proceedings of the 2nd annual conference on Information security curriculum development InfoSecCD '05*, september 2005.

[21] F. Dreher, "Designing an alternative for is 2002.4 information technology hardware and systems software course for an information assurance program," *Consortium for Computing Sciences in Colleges, Journal of Computing Sciences in Colleges*, vol. 21, 2005.

[22] B. Bogolea and K. K. Wijekumar, "Academic papers: Information security curriculum creation: a case study," *Proceedings of the 1st annual conference on Information security curriculum development InfoSecCD '04*, October 2004.

[23] L. Wilkens, B. B Ramamurthy, M. Olan, A. Kumar, K. Harmeyer, and L. D'Antonio, "Emerging areas in undergraduate computer science education: panel discussion," *Journal of Computing Sciences in Colleges*, vol. 20, february 2005.

[24] S. Azadegan, M. Lavine, M. O'Leary, A. Wijesinha, and M. Zimand, "An undergraduate track in computer security," *Proceedings of the 8th annual conference on Innovation and technology in computer science education ITiCSE '03*, vol. 35, June 2003.

[25] P. Cooper, "Pedagogy: Speciation in the computing sciences: digital forensics as an emerging academic discipline," *Proceedings of the 2nd annual conference on Information security curriculum development InfoSecCD '05*, September 2005.

[26] P. Wagner and Wudi, "Designing and implementing a cyber war laboratory exercise for a computer security course," *Proceedings of the 35th SIGCSE technical symposium on Computer Science education*, vol. 35, pp. 402–406, 2004.

ISBN 9-9999-9999-9/99/ $20.00 ©2007 IEEE