ABSTRACT

In this paper, we design and expand the highly successful Information Assurance (IA) program through education and training opportunities in digital forensics for students in other disciplines, and for local law enforcement professionals. Faculty development efforts will focus on the formation of a rich, lab-based teaching environment for instruction and applied research in digital forensics technology. In this project, two academic departments, Computer & Information Sciences (CIS), and Sociology and Criminal Justice (SCJ), will develop a cross-disciplinary computer concentration in digital forensics that positions students for professional certification; this concentration is suitable for undergraduate students and law enforcement professionals.

Categories and Subject Descriptors

General Terms
Management and Security

Keywords
Digital forensics, hands-on lab, cross-disciplinary, active learning, learning by doing

1. INTRODUCTION

The number of computer security incidents is growing exponentially and society’s collective ability to respond to this crisis is constrained by the lack of trained professionals [4]. Digital forensics (DF) plays an important role in crime reconstruction. Currently, the incidents of security breaches reported to federal agencies and to the U.S. Computer Emergency Response Team have increased dramatically. New challenges in the field create new opportunities for academia to develop new programs that will meet both the job markets’ and the students’ needs [8].

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. InfoSecCD’10, October 1-2, 2010, Kennesaw, GA, USA. Copyright © 2010 ACM 978-1-60558-661-8/10/10...$10.00.

For most college students, social networks are very popular forums that connect communities of people together. User privacy protection is a major issue in social networks. The State of the Internet 2009 report [20] found that the most notable online threat was rogue/fake security software, major search engines, social networks and Web 2.0 threats. Cyber-criminals have made a business out of attacking popular online sites. Search engines like Google and Yahoo, or social networking sites like Twitter or Facebook appeal to these criminals. For example, recently, a diamond ring ad that was posted on Craigslist lead to a deadly home invasion [21]. Cyber-crime poses a new challenge. Making students IA-aware, regardless of their field of study is a big challenge. It is critical to educate college students on the importance of protecting their privacy in social networking. This challenge reflects the reality that IA is interdisciplinary, drawing from multiple fields, such as computer science, criminal justice, engineering, management science, systems engineering, accounting, public administration, criminology and security engineering.

This presents a twofold task for digital forensics education: (1) it is critical for digital forensics awareness for criminal justice majors and other students who are interested in IA-awareness at Florida A&M University; (2) it is an urgent need for state and local law enforcement to have digital forensics professionals [1].

This curriculum is being proposed to expand the capacity of the IA program to a certificate in digital forensics, to meet the demand from CIS majors [12], and to move towards cross-disciplinary programs with Sociology and Criminal Justice (SCJ) and other disciplines. This curriculum focuses on academic courses that will help students obtain certifications and entry level positions in digital forensics. Also, this proposed curriculum program will provide training and support, while offering local and rural law enforcement departments value-added digital forensic consulting. In addition, we address faculty development for implementing this program as well.

This paper is organized as follows: Section 2 gives an overview of the existing digital forensics program at Florida Agricultural and Mechanical University (FAMU) and present current status of DF/IA at FAMU. Section 3 proposes detail plans for the certificate program in digital forensics: this includes curriculum development for other majors at FAMU, laboratory establishment and faculty development at FAMU. Section 4 describes student learning model. Conclusions are made in Section 5.
2. BACKGROUND

The job market for digital forensics is in big demand from state and local law enforcement [26]. A recent Department of Justice survey indicated that nearly 60 percent of American businesses have detected one or more cyber attacks. However, 90% of law enforcement agencies employ less than 50 sworn personnel (see Table 1). The challenge for law enforcement is to find professionals who have digital forensics training. Given the rise of crimes involved in computers and the internet, demands for digital forensics professionals are high especially for small law enforcement agencies since they are less likely to have specialists in digital forensics. Providing those skills for a broader populace will make FAMU students more marketable.

Table 1. State and local law enforcement

<table>
<thead>
<tr>
<th>Agencies personnel*</th>
<th>sworn</th>
<th>number</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>17,784</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>1,000 or more</td>
<td>77</td>
<td>0.4%</td>
<td></td>
</tr>
<tr>
<td>500-999</td>
<td>83</td>
<td>0.5%</td>
<td></td>
</tr>
<tr>
<td>250-499</td>
<td>203</td>
<td>1.1%</td>
<td></td>
</tr>
<tr>
<td>100-249</td>
<td>669</td>
<td>3.8%</td>
<td></td>
</tr>
<tr>
<td>50-99</td>
<td>1,177</td>
<td>6.6%</td>
<td></td>
</tr>
<tr>
<td>25-49</td>
<td>2,237</td>
<td>12.6%</td>
<td></td>
</tr>
<tr>
<td>10-24</td>
<td>4,124</td>
<td>23.2%</td>
<td></td>
</tr>
<tr>
<td>5-9</td>
<td>3,623</td>
<td>20.4%</td>
<td></td>
</tr>
<tr>
<td>2-4</td>
<td>3,453</td>
<td>19.4%</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1,907</td>
<td>10.7%</td>
<td></td>
</tr>
</tbody>
</table>

*source 2000 DOJ statistics [23]

Our department has a positive track record in information assurance education. Since its introduction in our department, the IA track has enjoyed the demand and throughput shown in Table 2. Additional IA courses have been introduced to meet the growing demand for digital forensics and for elective courses suitable for other majors such as criminal justice. This paper reports on our efforts to increase the capacity of the IA program to meet the demand from CIS majors, and to move towards cross-disciplinary programs within the areas of science, technology, engineering and mathematics (STEM) and other disciplines.

Table 2. Demand for IA Courses at FAMU

<table>
<thead>
<tr>
<th>IA Courses</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intro to Computer Security</td>
<td>30</td>
<td>24</td>
<td>30</td>
<td>18</td>
<td>27</td>
</tr>
<tr>
<td>Network Security &amp; Cryptography</td>
<td>17</td>
<td>22</td>
<td>11</td>
<td>16</td>
<td>11</td>
</tr>
<tr>
<td>Applied Security</td>
<td>38</td>
<td>21</td>
<td>40</td>
<td>17</td>
<td>15</td>
</tr>
<tr>
<td>Digital Forensics</td>
<td>N/A</td>
<td>N/A</td>
<td>12</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>#Certificates</td>
<td>5</td>
<td>10</td>
<td>29</td>
<td>7</td>
<td>6</td>
</tr>
</tbody>
</table>

We are experiencing increasing demand from non-CS students who want to earn an IA certificate. Because these students do not have the full complement of IT courses that CS students bring to the IA courses, we face the challenge of providing these students a meaningful course experience, without first requiring them to complete a long sequence of preparatory courses. The two strategies we currently employ are collaborative learning activities involving mixed teams of CS and non-CS students, and the use of hands-on labs.

3. DIGITAL FORENSICS CURRICULUM

3.1 Current Digital Forensics at FAMU

Since Fall 2007, CIS annually offers a digital forensics course for CIS undergraduate students. A graduate-level course was offered Spring 2008. These courses are very popular with a total enrollment of approximately 70 students [22]. This course will be offered again during Fall 2010. Open sources are used, such as the Sleuth Kit (http://www.sleuthkit.org/), trial version of Forensic Toolkit from AccessData Company (FTK) [15] to make students complete hands-on labs. Some cases for hands-on labs come from the Honeynet Project Challenges (http://www.honeynet.org) as digital forensics tools [7, 8].

However, those courses in Table 2 are suitable for CS-majors. It is impossible for non-majors to take all those courses without CS prerequisites. It is necessary to offer IA courses to bridge those gaps for non-majors so that non-CS-majors can take those classes as well.
The following section will show how FAMU will implement this program for other majors.

### 3.2 The Proposed Digital Forensics Curriculum

The objective of this collaborative project is for FAMU to create a digital forensics certificate program following the examples from the Dakota State University [5] and West Virginia University (http://www.lesee.emr.wvu.edu/forensics/). However, both of them are designed for graduate programs or for CS-majors only.

We have to design our curriculum for CS and other majors as well. Thus, the activities in this section are intended to enhance FAMU faculty's capability to offer required courses for digital forensics. The goal of this paper is to develop an interdisciplinary undergraduate digital forensics certificate program at FAMU. It is proposed to develop complementary digital forensics courses at FAMU. In Table 3, the development of a couple of undergraduate interdisciplinary digital forensics courses is proposed. The certificate requires 18 credit hours (6 courses) through required core curriculum courses.

#### Table 3. FAMU Undergraduate Digital Forensics Certificate Program

<table>
<thead>
<tr>
<th>Course Name</th>
<th>Courses Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS4360: Intro to Computer Security</td>
<td>The main issues and main threats in computer security are introduced. Privacy and integrity of data together with the availability of computer resources need to be guaranteed.</td>
</tr>
<tr>
<td>CIS 4362: Network Security &amp; Cryptography</td>
<td>This course addresses issues of network security from authentication to non-repudiation. It will address the fundamental theories of network security including public and private key cryptographic techniques.</td>
</tr>
<tr>
<td>CIS 4363: Applied Security</td>
<td>This course introduces issues of information security. Also addressed are the fundamental theories of security policy, security vulnerability and protection. The material will relate to current issues that affect day to day computing.</td>
</tr>
<tr>
<td>CIS 4385: Digital Forensics</td>
<td>This course introduces students to a variety of digital evidences and software. Emphasis is placed on using common media analysis tools and techniques to locate and recover digital evidences in a forensically sound manner.</td>
</tr>
<tr>
<td>CJL 4xxx Cyber Law</td>
<td>This course offers the legal (and ethical) aspects of managing technology in cyberspace. The objective of this course is to provide computer science and criminal justice students with a legal overview of the impact of cybercrime</td>
</tr>
<tr>
<td>CIS 4xxx Computer Forensics project</td>
<td>The course will be project oriented and focus on real-world case study that can be involved computer and network forensic analysis [13,14,15,16].</td>
</tr>
</tbody>
</table>

These six courses cover the major areas of study.

During the two-year period, FAMU will develop four courses that will lead to an undergraduate certificate at the Intermediate level. The intent is to attract students into the pipeline and to position them for professional as well as academic futures [11, 12]. Two courses are for certificate programs and the other two are for digital-forensics-awareness programs. The first course CGS 2xxx will be mainly offered for SCJ and other majors so that the students can have enough computer knowledge to advance to DJL/CGS 3xxx—Cyber crime.

During the next year, FAMU will establish a digital forensics teaching lab that extends our NSF-funded security lab and mirror virtual labs from successful examples with respect to hardware and software [10, 13]. All Arts and Science majors at Florida A&M University are required to have a minor in order to be eligible for graduation. Minor programs offered within the College of Arts and Science typically require that the student completes 18 hours (6 courses).

Typically, Criminal Justice majors select sociology, anthropology, psychology, pre-law, public administration, political science, social work, history, economics, foreign language or English as minors. With departmental approval, Criminal Justice majors who are participating in the Adrian Project (IRS Criminal Investigation Program) are allowed to take accounting courses from the School of Business for a minor in accounting. The inclusion of a Digital Forensics minor enhances the minor options that are already available for Criminal Justice majors, but, more importantly, a Digital Forensics minor will make our students more marketable for a career in an area of criminal justice that is in high demand.

The objective of this course is to provide computer science and criminal justice students with a legal overview of the impact of cybercrime. The structure of the criminal justice program can easily accommodate a digital forensics minor. Criminal justice students must complete 60 hours of general education courses. Recently, the criminal justice curriculum was modified to include computer literacy course—CGS 2060C (Computer Literacy I) as a requirement for all criminal justice majors. CGS 2060C is counted towards the general education requirements. Also, although CCJ 2010 (Introduction to Criminal Justice) is required for all criminal justice majors, it is a general education prerequisite. In addition to the 60 general education hours, the 18 hour minor and 30 hours of criminal justice courses, criminal justice majors have 12 remaining hours that can be used towards an internship or additional courses. Given the fact that the minor requirement has already been implemented in the criminal justice curriculum, the option of a Digital Forensics minor will not negatively impact the university’s 120 hour rule.

### 4. LEARNING MODEL

The nature of digital forensics is interdisciplinary. Digital forensics has become a basic skill that all criminal justice students need. This project will identify basic digital evidence competencies that will enhance criminal justice students’ performance and broaden their opportunities for employment, advanced study and career growth. The CIS Department will serve as a catalyst for identifying digital forensics competencies and developing courses to meet their needs. Additionally, the CIS Department will support the SCJ faculty’s development to promote awareness of digital forensics technology. It is expected that once SCJ faculty members begin teaching cyber law and cyber crime related courses, the research collaborations will commence between CIS and SCJ.
Certain techniques and procedures have to be established in the quest of evidence identification, preservation, extraction, documentation, and interpretation. Individual lab work is designed to help students understand these procedures and practice them first hand. Knowing and understanding the tasks a computer forensic professional may be called to do, provide a sufficient guide as to how to design a lab. Some lab assignments may include: (1) Acquiring an image for analysis; (2) Recovering deleted data; (3) Dead and Volatile Analysis; (4) Removable media analysis; (5) Utilizing operating system’s preinstalled tools e.g., event log and event viewer; (6) Password and encryption methods; (7) Decrypting files; (8) Identifying images and steganography; and (9) Finding hidden data [23].

Several different labs will be designed to accommodate various difficulty levels and students’ majors—computer majors versus criminal justice majors or any other majors. The labs will express, the different scenarios that a forensic examiner may experience in the field—law enforcement cases versus cooperate type cases—and encompass samples of real cases.

To teach cyber law and cybercrime more effectively, a more interactive, hands-on approach, where current news reports and case examples can be reviewed and discussed in class would facilitate student learning [20]. The computer labs where these classes will be taught should have access to a permanent projection system where case studies and news reports can easily be presented in class. Also, in order to ensure that the most recent rule of law, as it relates to Cybercrime is covered, it is necessary that students have access to West Law. Currently at Florida A&M University, West Law is only provided for the law students. Having West Law available in the lab will ensure that the most recent rule of law is learned.

While Cyber Law will primarily address legal issues pertaining to cyberspace and the prosecution of cyber-criminals, Cyber Crime will address various aspects of crimes that are committed in cyberspace. The topics covered in Cyber Crime will range from theoretical explanations to specific types of crime that are carried out in cyberspace by cyber-criminals (e.g., cyber bullying, cyber stalking, identity theft, cyber terrorism, etc.). The computer lab will serve as an effective tool to engage students in a hands-on approach to study the crimes committed in cyberspace. For example, most students actively communicate through social networking sites; however, they are often not aware of the fact that they can leave themselves open to criminal victimization through the information that they post. The lab would serve as an effective teaching tool to demonstrate ways to reduce criminal victimization in social network environments. In class critiques and discussions on active sites can serve to be more effective than mere textbook discussions.

Course projects can also be designed where students can select an electronic device and conduct a threat modeling of the device. Again, the lab would serve as an environment where students can collaborate on assigned projects for this course. Experts in cybercrime from local law enforcement agencies will be invited as guest lecturers for this course. The labs would be beneficial in that it will allow these professionals to demonstrate various aspects of cybercrime through the use of an online teaching computer lab [21].

4.1 Hands-on Labs

Certain techniques and procedures have to be established in the quest of evidence identification, preservation, extraction, documentation, and interpretation. Individual lab work is designed to help students understand these procedures and learn some fundamental techniques, especially in areas where cyber crime is central. It is believed that the success of this project requires a true transfer of computing technology from the CIS faculty to SCJ faculty, and that this transfer is actually a two-way street, or cross-training: CIS faculty must learn concepts of the criminal justice discipline as well.

4.2 Active Learning

Active learning refers to techniques where students do more than simply listen to a lecture. Active learning results in a deeper and more integrated understanding of concepts, as well as significant improvement in student retention in degree programs. Engaged students remember concepts longer, enjoy the learning process more, and are more likely to continue. Gaming technology, which emphasizes engagement, provides an additional tool for implementing active learning.

The skills for a digital forensics professional fall into the areas shown in Figure 1 [25]. This education is inter-disciplinary, combining criminal justice and computer sciences; therefore, we have to ensure that our students acquire the competencies to work effectively in both areas.
4.3 Learning by Doing

When students with limited computing background enter the IA field, they face a steep learning curve. Hands-on labs that employ game playing help students to quickly grasp core content and topics [24]. Active learning refers to techniques where students do more than simply listen to a lecture. Hands-on based labs, which emphasizes engagement, provides an additional tool for implementing active learning.

The “learning tree”, shown in Figure 2, illustrates how students learn IA concepts effectively. The procedure of active learning begins with the initial exposure, where the student witnesses the use of new concepts to explain or explore an IA issue in a virtual environment. Interested students will be afforded additional opportunities to learn to apply IA concepts to solve a real-world problem or do an experiment. The next level of learning is adaptation, where one has become familiar enough with IA concepts/measure to find solutions for their real-world specific security problems. The application and adaptation stages mark the onset of research. Advanced research involves creating new IA technology, e.g., creating new IA models or new IA measures.

In this program, active learning is achieved by doing hands-on labs. Non-major students will learn IA easily by exploring real-world cases [9]. Hands-on labs, such as decrypting files or password cracks, can quickly provide scenarios to show that disastrous results will occur when poor choices for passwords are used. Finally, students will master the IA concepts and tools they learn to solve real-world problems by themselves. Through the use of hands-on labs, they will acquire the ability to creatively work out complicated IA problems.

5. CONCLUSIONS

In this paper, a program has been detailed which strengthens and expands digital forensics education. The certificate program leverages the strengths of both departments CIS and SCJ at FAMU, resulting in a program that draws inter-disciplinary departments working together allowing them to synergistically complement one another. The specific objectives of this project include:

- Establish a cross-disciplinary undergraduate certificate program in digital forensics at FAMU;
- Increase the number of CIS and other discipline graduates who are digital-forensics-aware;
- Develop and implement a set of hand-on labs for different levels of undergraduates who will take digital forensics certificates;
- Expose more minority students to digital-forensics-aware at FAMU; and
- Establish a sustainable collaboration between CIS and SCJ for education, and professional development in Digital Forensics.

The success of this project requires a true transfer of computing technology from the CIS faculty to SCJ faculty and that this transfer is actually a two-way street, or cross-training. The project leverages the strengths, capabilities, and needs of all participating departments.

The resulting program will produce students who are ready to seamlessly proceed into the information forensics workforce. The availability of a digital forensics minor for criminal justice majors at Florida A&M University will not only increase their marketability, it will enhance the offerings that are available to them as well. While this program will certainly benefit those students who choose digital forensics as a minor, it will undoubtedly prove itself to be beneficial to federal, state and local criminal justice agencies that seek qualified applicants who are highly educated and trained in the field of digital forensics.

6. ACKNOWLEDGEMENTS

This work has been supported in part by U.S. Department of Education grant P120A080094. Thank the anonymous reviewers for a number of comments and suggestions that helped to improve the paper.

7. REFERENCES


[18] FTK (Forensic Toolkit), http://www.accessdata.com/


