Information Systems Forensics: a Practioner's Approach

Christopher Malinowski
Computer Science and Management Engineering
CW Post Campus, Long Island University
720 Northern Blvd., Pell Hall 222
Brookville, NY 11548, USA

1. INTRODUCTION

Recently many institutions have been subjected to a decline in the enrollment of students within the disciplines of computer science and information systems studies.

The reasons for this decline may be attributed to a variety of causes generated from either end of the educational assembly-line: the student recruitment and retention process, or the industry in which the students eventually find themselves. Figures cited from the Bureau of Labor statistics[1] indicate that over the past four years employment has decreased by over twenty percent for analysts, programmers, and support specialists. Conversely the market apparently has improved for software engineers (7%), network and systems administrators (32%), and managers of computer and IS (54%). Network systems and data communications analysts have remained relatively flat (down 1%).

For a variety of reasons, educational institutions are constantly reviewing and updating their programs in order to reflect market and industry needs as well as to market the program to potential students. Factors which *can* be controlled should be examined in order to determine if programs can be altered in order to attract and retain the student population required to make the programs viable

Unfortunately a myriad of factors cannot be controlled. The recent trend to "downsize" and outsource information systems jobs has affected enrollment to some degree. Restrictions for I-20 visa issuance have apparently affected the number of foreign students in my institution since the tragedy of September 11th impacting graduate enrollment. The incoming undergraduate students' skills in mathematics and "hard sciences" have apparently declined. The result is that IS instructors find it difficult to demonstrate building a front-end input form in order to calculate tips or taxes, or even convert temperature from Centigrade to Fahrenheit when some students struggle with the fundamental math involved.

While hopefully most of the undergraduate students in a class are *not* struggling to such a degree, the decision needs to be made: should the pace of instruction match the skills of most students, or do we allow these students to fail out? Perhaps unstated is the economics of the situation; should we fail out too many students, from where will we obtain the enrollment in order to sustain the program?

In a similar vein, our programs have historically witnessed a movement in which students leave a more rigorous computer science program for an information systems program. Likewise, students may also switch from information systems to an information management program offered, which includes courses such as support service environments.

One alternative which allows us to serve the students by providing an education, enhancing their marketable value and serving the industry, is to consider instituting a 'computer forensics' program.

Of late such programs have been appearing in various colleges. Essentially these students can function as computer and/or network security specialists within an organization, or leverage their education in order to place themselves with a governmental agency.

Educational concerns can be allayed, as the topics covered span a gamut from computer science into information systems, and even include ethics and law. On the undergraduate level, this could readily be embraced as a rounded program.

Technical, operational, and economic feasibilities must be examined prior to establishing such a program. Insofar as each institution has different concerns in these regards, these questions are not addressed in this paper.

Whether a program is named "network security concentration", or "computer security" we need to establish precisely what the range of skills we seek to teach will be. One method is to examine the tasks routinely performed in industry settings and utilize these as skill goals for the student.

2. PRIVATE SECTOR VERSUS PUBLIC SECTOR

Depending upon the nature of the business, as well as the size of the organization, corporate structures may employ individuals to monitor, test, and routinely enforce corporate IT security policy. The size of the organization may dictate whether the individual is a staffer dedicated to these functions, or is routinely assigned to IT or some other unit, and performs these security functions on demand or as required.

Taking this into account we should consider having our curriculum balanced in order to cover a variety of computer science and information systems topics. On an undergraduate level, narrowly focusing our curriculum would be comparable to conducting a physics curriculum in which the focus is solely nuclear physics. The student would lack the malleability to learn new topics: a crucial ability when one considers the rate at which technology is changing.

Graduate students should already have a developed sense of the industry and the technology, and ideally focus their efforts more narrowly. Care should be given in considering admission of graduate candidates not having a "rounded" and *formal* information systems background.

The experiences of the faculty in CW Post have indicated that graduate IS candidates do not necessarily possess the requisite knowledge base, despite the fact that they have worked in the industry for substantial periods of time. The manner in which we deal with this impediment may resolve issues in accepting candidates whom otherwise might otherwise not be accepted into our programs.

Public sector concerns differ to some degree. In many cases, personnel performing these tasks of necessity come from within the existing personnel system. Often these personnel are not formally trained in many (or any) aspects of the required tasks, and perform tasks under supervision and receive training "as they go."

Other public agencies have the ability however to select candidates for narrowly defined positions within their agencies. The focus of the position within a public sector agency is to locate skillsets which are more narrowly defined along with field experience. Failing that, a selection for general aptitude (information systems) skills with the potential for skill development within the organization may be acceptable.

Examination of the target job markets should provide a range of the skills to be encompassed within a curriculum.

While many employers in the private sector encourage training program certifications, often these certifications may be narrowly defined to a particular vendor's equipment or service. The value of examining the certification however does lie in determining the education required to match the level of the training.

A general or broad certification relies on a body of knowledge which is deemed to represent the current technology, and for which the student has demonstrated mastery in the concepts and protocols involved in that technology, such as the CISSP (Certified Information Systems Security Professional) certification.

CISSP certification covers ten knowledge areas[2]:

- Access Control Systems & Methodology
- Applications & Systems Development
- Business Continuity Planning
- Cryptography
- Law, Investigation & Ethics
- Operations Security
- Physical Security
- Security Architecture & Models
- Security Management Practices
- Telecommunications, Network & Internet Security

If indeed, these concepts underlie the technology involved, the mastery of the concepts should enable the student to possess and understanding of the technology.

In contrast, promulgating a curriculum which follows the recommendations of an established organization may enhance the *prima facie* value and marketability of the curriculum.

One possibility to pursue in the future is to obtain an NSA (National Security Administration) certification as a Center of Academic Excellence. Pursuit of this certification is contingent upon the direction of future program development. The standards for this certification are grounded in the guideline provided by the NSTISS[3]. Certification by a recognized agency indicating adherence to a set of standards can be an incentive for potential students and validate the offered program.

Yasinsac, ET. al.[4], offer a matrix of "roles" in the disciple of computer and network forensics. This "CNF" matrix describes a progression of increasing complexity of skills and depth of understanding in the subject matter.

Essentially the four roles address various needs of law enforcement, business and academia vis-à-vis computer and network forensics. Viewing these positions as the goals/deliverables of any forensics curriculum, we can proceed to define a program, or alter an existing one in order to accommodate a forensics program. Outlined in the same publication are educational cognates for industry training certifications, such as the A+ or .Net + certifications.

A "CNF technician" embodies the basic skills required to perform first responder duties to incidents as well as perform basic data duplication and recoveries. The education requirements are all introductory level courses in forensic science, computer science, operating systems, hardware and an introduction to criminal and civil law. The training reflects the formal education, such as A+ training, Net+ training, and basic computer seizure and data recovery. This role can provide a basis for curriculum development.

The "CNF policy maker" is concerned with Information Assurance (IA), and should have knowledge of enterprise architecture, a deeper appreciation of forensic science, and information and knowledge management.

A "CNF professional" extends the SKA (skills, knowledge, and ability) of the technician in the areas of information systems, computer science, and the legal world. The data recovery skills should be more developed that those of the technician.

And finally, the "CNF researcher" should be capable of extending the body of knowledge, having experience in the arena of computer forensics.

These areas can be mapped out to match a program in either an undergraduate or a graduate forensics program with the demarcation between the graduate and undergraduate occurring in the "professional" stage of the role progression.

3. GRADUATE PROGRAM

Currently CW Post offers three Masters Degree programs in the Computer Science Department: Information Systems (ISY), Management Engineering (MGE), and Computer Science Education / User Support (CPE). No program exists for Computer Forensics.

Graduate ISY students are required to take Networks and Internetworking, along with Enterprise Networks. On rare occasion a special topics elective in Network Vulnerabilities is offered. As a result, students have expressed interest in taking additional network courses, as well as exploring the realm of network or computer forensics.

If we examine the graduate programs, one of the most evident weak points is the SKA of the candidate student.

While my experiences in CW Post have taught me that many of the graduate students in the Information Systems program are interested in network security and computer forensics in general, for the most part many do not have the prerequisite skills in order to properly put together a section of a class. How then, would we address the initial economics of the program?

At CW Post, the graduate Information Systems program in our department allows students to take "pre-core" courses, obtaining the *formal* education in the subject matter area. This benefits the students in that they are not precluded from pursuing studies by dint of not having completed an IS or CS undergraduate degree. The practitioners with working knowledge can gain the formal knowledge, enabling them to be assured of successfully completing the program.

Since it is currently unlikely that graduate candidates will have the prerequisite information when applying for a graduate study of computer forensics, the program must include a set of courses which would allow the student to "bootstrap" himself into the graduate level courses. While currently there is no "computer forensics" program at our institution, setting the groundwork for such a program, while at the same time supporting the existing programs is a key element of any plan to institute a computer forensics program.

Bearing in mind that the graduate student requires the SKA of the CNF technician, there would be three possibilities for any "pre-core" work for the graduate level students within our institution:

- Addition / modification of course(s) in an existing program
- Intro level course may be satisfied by undergraduate level subject matter currently available
- A student demonstrates formal education from other institutions or certification in subject matter areas

The required courses in the current graduate programs do not address the desired graduate requirements of a graduate level forensics program, nor even the undergraduate (CNF technician paradigm) level.

Establishment of a graduate program in computer and/or network forensics is dependent upon candidate students having the required skills prior to commencing the program of study. The most expedient possibility, while minimizing risk, is to establish the undergraduate track or program. This track may very well provide a mechanism for graduate students to obtain the knowledge of a CNF technician.

With an undergraduate track in place, if a "pre-core" course is lacking, a graduate student is allowed to satisfy the requirement by enrolling in the same course along with undergraduates (depending on the subject matter). For example, instruction of a coding course (Java, C++) might have the same presentation for both graduate as well as undergraduate students. We have been able to do this on occasion by opening up evening sections of an undergraduate course. For the graduate students to take advantage of this possibility the appropriate undergraduate courses need to be scheduled appropriately.

Finally, if a pre-core course is satisfied outside the institution, the student is deemed to possess the knowledge necessary to proceed onto the graduate level courses.

Candidates claiming to have either "real-world" or certificate experience require substantiation of their knowledge prior to waiving a pre-core requirement. In the past, students having claimed a waiver of a pre-core course have resulted in time consuming reviews in class sessions rather than covering new ground and material.

4. UNDERGRADUATE PROGRAM

The undergraduate programs within the Department currently include computer science (CSC), information systems (INS) and Information Management Technology (IMT).

As it is currently structured, our IMT program presents the best opportunity for establishing those courses addressing the "CNF technician" role due to its flexible elective schedule.

5. CONSIDERATIONS

Hal Berghel[5] asserts there is a difference between the fields of Computer Forensics and Internet (network / internet) Forensics. Part of the delineation resides in the level of the different skills involved in performing the tasks of each discipline. Another difference pointed out by Berghel is more subtle: the tools required to perform network forensics are in many cases the same tools used by the hacker / cracker, whereas the computer forensics tools are not, and in many cases concern the physical aspects of the target system.

This difference is important when developing a program for a variety of reasons. While the program to be developed depends on the goals, it also depends on the starting point (students). In other words, we need to identify the resources already in place, or those that can be leveraged with minimal impact.

New resources required in order to implement such a program must be identified and considered. In our case, the initial resource required in order to implement a new track are in place. Timing of the new track is concurrent with computer lab updates, allowing us to utilize the outgoing hardware platforms for the new courses.

Initially, the courses can be instructed by one or two instructors without impacting current programs.

Bearing this in mind, the most expedient alternative which is being pursued at CW Post is to establish a networks concentration or track for the undergraduate program (IMT) comprised of several courses that are network and network security based.

These courses, while providing a concentration (or "track") for an existing program, also serve to lay the foundation for an undergraduate computer / network forensics program. There also exists a potential that these courses could fulfill "pre-core" requirements for the graduate candidates should the time of day in which the class is offered prove advantageous to the graduate candidates.

6. PROPOSED NETWORK TRACK

Based on a series of books published by Course Technology, the proposed undergraduate track for networking is as follows:

Network Security Fundamentals

1. Security Overview
2. Authentication
3. Attacks and Malicious Code
4. Remote Access
5. Email
6. Web Security
7. Directory and File Transfer Services
8. Wireless and Instant Messaging
9. Devices
10. Media and Medium
11. Network Security Topologies
12. Intrusion Detection
13. Security Baselines
14. Cryptography
15. Physical Security
16. Disaster Recovery
17. Computer Forensics / Other Topics

Intrusion Detection

1. Firewall Planning and Design
2. Developing Security Policy
3. Configuration Strategies
4. Packet Filtering
5. Proxy Servers / App Level Firewalls
6. Authenticating Users
1. Encryptions and Firewalls
7. Bastion Hosts
8. VPN Setup
9. Building Firewall and VPN
10. Administration

"Hacker's Perspective" / Vulnerabilities

Examination of various methodologies to exploit network and system vulnerabilities

1. Loopholes
2. Concept behind loopholes
3. Exploits
4. Common Tools
5. Detection and countermeasures
6. Incident Response

Web Security for Administrators

1. General Security
   a. Information Security
   b. Processes
   c. Threats
   d. Encryption
2. Network Security
   a. Fundamental Network Security
   b. Network Architecture
   c. Security Architecture
3. Operating System Security
   a. Fundamentals
   b. .NET security
   c. Threats and solutions
4. Security Testing
   a. Policy Compliance
   b. Testing methodology

Introduction to Computer Forensics

1. Computer Forensics as a Profession
2. Computer Investigation Process
3. MS Operating Systems, Boot Processes and Disk Structures
4. Macintosh and Linux OS, Boot Processes and Disk Structure
5. Investigator's Office
6. Current Tools
7. Digital Evidence Controls
8. Crime / Incident Scene Processing
9. Data Acquisition
10. Computing Forensic Analysis
11. Email Investigations
12. Graphic Image Recovery
13. High Tech Reports
14. A Forensic Application Overview

Students will have already had a course in Introductory Data Communications and Networking. Care must be taken to tailor the

Data Communications and Networking course to include the elements which are listed in the syllabi of the network track courses, such as remote access, wireless technology, and the underlying protocols (SMTP, POP, FTP, TCP/IP, and etcetera).

Target students for this track, although required to take the Intro Networks course, are not currently required to take an operating systems course. While one of the track courses addresses *aspects* of operating systems such as Windows, or Linux, other aspects are not made known to the students formally.

Another area, which is not readily apparent, is the lack of skills in computer literacy. The skills required by the students taking this track of coursework must surpass the basic skills of the computer literacy course. If we strive to emulate the CNF technician model for the undergraduate students as a goal, then we must examine typical tasks performed by the technician in the field that are considered day-to-day work.

Coding, although not evident in the comprehension of network fundamentals, does factor in as a requirement at some point. Students examining web pages should be capable of understanding the underlying JavaScript coding in order to determine the behavior of web pages visited and how they may affect systems having visited those sites.

Due to the potential volume of information provided as part of a forensic examination of a network, students need to be capable of handling that information. If the information is properly formatted, then standard applications or even office productivity suites may be capable of processing the information. Should this not be the case however, the student requires the ability of data manipulation data in order to directly obtain the information or convert the data into an acceptable format for processing with existing tools.

Institution of this track within the program may allow for expansion into a computer and network forensics program.

If we examine the new concentration, we can determine that the CNF technician paradigm has been reduced to NF technician. The initial focus is on the network / internet aspect of forensics.

The result is that we have a series of courses which are available as required courses for IMT students in the networks track, or elective courses for the CSC or INS students. If we desire to establish a fourth program (Computer and Networks Forensics) within the Department, the track serves as a litmus test, and will be in place at such time when the Computer Forensics component can be developed and sanctioned officially as a program. Essentially we could be phasing in an entire program, using networks forensics as a milestone in our project.

The rationale for providing the computer forensics overview course is that networks reside on platforms, and are not discrete entities. An understanding of the underlying platform is required for technicians in the field, and therefore for the undergraduate student. For example, the student may very well understand that the information required determining the cause of a network problem resides within either auxiliary or volatile storage on a platform. The nature of the *acquisition* of this information is critical to the field of forensics. Forensics resides in the application of technology in order to adhere to legal strictures.

7. COMMENTS ON PLANNED CONCENTRATION

The Course Technology series of texts was initially selected due to its comprehensive span of topics within the discipline, the readability of the text by undergraduates, and the ability to base exercises on readings. Redundancy in topics between texts is limited, as compared to potential overlaps in content when using texts by disparate authors not published in the same series.

The "vulnerabilities" course has been drawn from a variety of readings, as opposed to a supplied text. As the material presented requires an understanding of the communications protocols and basic operating systems, the course may also serve as an unofficial capstone course for the concentration.

For any of the courses, supplemental readings can be assigned as well as development of research areas in order to venture beyond the bird's-eye view of the texts.

Logistics problems need to be considered as they can be quite costly and prohibitive. These can include, but are not limited to, computer and networking components, software packages, staffing issues, maintenance issues and etcetera.

Some practical concerns of maintaining a lab may include:

- Physical space allocation for the network and lab
- Additional equipment to segregate and maintain the lab as well as allow exercises
- Access to "root" (privileged) capabilities on a system
- Legal liability
- Licensing of proprietary software
- Instructional staffing
- Lab staffing (dedicated person)
    - Workstation restorations
- Sharing of workstations by students
- Prolonged practical labs

Timing of the concentration was dependent upon the ability to put the physical components of a separate network into place; as one of the Department's computer labs was updated, the platforms were recycled into the network track. This allowed the Department to provide two small LANs, as well as sufficient PCs for students working in groups of three or fewer to develop their network skills.

One impediment is the ability to staff instructors for any such program. Typically, instructors carrying a typical course load are restricted in the number of courses they can teach. In addition, the subject matter is hardly one for which other members of the faculty may be cross trained. One possibility is to include industry experts as lecturers or adjuncts, provided that the syllabi are in accordance with the course content and the program as a whole.

Just as Computer Forensics can be put into a combined category of Computer and Network Forensics, some have suggested and even broader view: Data Forensics.

The implications are far reaching for those contemplating a program. Data Forensics deals with data resides, as well as the transmission of data. With Moore's Law shrinking daily, and the growth of newer technologies, the ability of data to reside on devices has expanded. Devices such as telephones can now function as computers, or become stores of data, in addition to being the means of transmission of data.

The practicalities of purchasing, maintaining, and instructing "data forensics" is overwhelming, and probably not feasible in an educational setting; these may be left for the professional or the researcher in the industry to pursue.

8. CONCLUSIONS

If we examine the planned concentration, we can determine that the CNF technician paradigm has been reduced to NF technician. The initial focus is on the network / internet aspect of forensics.

The result is that we have a series of courses which are available as required courses for IMT students in the networks track, or elective courses for the CSC or INS students.

If we desire to establish a fourth program (Computer and Networks Forensics) within the Department, the network track serves as a litmus test, and will lay the foundation if and when the Computer Forensics component can be developed and sanctioned officially as a separate program.

By reducing the scope of the initial program to a networks based track, we reduce the liability with respect to the resources required, the logistics, and the risk of establishing a new Computer and Network Forensics program as a "day one" program; instead the new program can be viewed as an extension of the existing supported network track.

Any program which hopes to remain viable must consider not simply the immediate costs, but also the recurring and new costs that will develop in order to successfully maintain the program.

By encompassing any such curriculum within the general considerations of Information Systems, we can hope to provide students with the capacity to learn with their discipline and a set of tools to enable them to seek placement in a job market that is growing and less likely to be 'relocated' elsewhere due to outsourcing concerns. Should this effort prove successful, then enrollment should increase, providing benefit both to the students as well as the institution.

9. REFERENCES

Azadegan, S. , M. Lavine, M. O'Leary, A. Wijesinha and M. Zimand, "An undergraduate track in computer security," 2003, Annual Joint Conference

Integrating Technology into Computer Science Education, Proceedings of the 8th annual conference on Innovation and technology in computer science education, pp. 207-210.

Bacon, Thomas and Rahul Tikekar, 2003, "Experiences with developing a computer security information assurance curriculum," Journal of Computing Sciences in Colleges, v.18, no.4, pp. 254-267.

Campbell, P, B. Calvert, and S. Boswell, Security+ Guide to Network Security Fundamentals, 2003, Thomson-Course Technology

Crowley, Ed, "Information system security curricula development," Proceeding of the 4th conference on Information technology curriculum, 2003, pp. 249-255

Holden, Greg, Guide To Firewalls and Network Security: Intrusion Detection and VPNs, 2004, Thomson-Course Technology

Mackey, D., Web Security for Network and System Administrators, 2003, Thomson-Course Technology

Nelson, W., A. Phillips, F. Enfinger and C. Stuart, Guide to Computer Forensics and Investigations, 2004, Thomson-Course Technology

NSTISSI, "No. 4011 – National Training Standard for Information Systems Security (INFOSEC) Professionals," 1994.

Tikekar, Rahul and Thomas Bacon, 2003, "The challenges of designing lab exercises for a curriculum in computer security", Journal of Computing Sciences in Colleges, v.18, no.5, pp. 175-183

Troell, Luther , Yin Pan and Bill Stackpole, 2003, "Forensic Course Development", Proceedings of the 4th Conference on Information Technology Curriculum, pp. 265-269

Yasinsac, A., R.F. Erbacher, D.G. Marks, M.M. Pollitt and P.M. Sommer, "Computer Forensics Education," 2003, Security & Privacy Magazine, IEEE, v.1 no. 4, pp. 15-23

[1] McGee and Chabrow, "Tech-Job Upheaval", Information Week, Aug 2, 2004

[2] International Information Systems Security Certification Consortium, Inc., http://www.isc2.org/cgi/content.cgi?category=19

[3] National Security Telecommunications and Information Systems Security Standards (NSTISS), Committee on National Security Systems: http://www.nstissc.gov

[4] A. Yasinsac, "Computer Forensics Education," Security & Privacy Magazine, IEEE vol 1, no. 4, pp15-23

[5] H. Berghel, "The Discipline of Internet Forensics", Communications of the ACM, vol. 46, Issue 8, pp 15-20, 2003