Proceedings of the 8th Colloquium for
Information Systems Security
Education
West Point, NY June 2004

Is it Safe?
Information Security Education: Are We Teaching a Dangerous Subject?

Patricia Y. Logan Ph.D., *Associate Professor, Marshall University Graduate College,* and Allen Clarkson, *Graduate Student, Marshall University*

Abstract – Teaching computer science at the university level presents areas of potential conflict with computer services and their responsibility for delivering a secure network environment. This conflict is particularly evident in the case of computer security study where the use of course-related tools may violate Acceptable Use Policies (AUPs) for the university network. Computer Science departments need to be accountable to the university community at large for the tools of instruction in these classes – particularly tools that will violate policies, such as key loggers, password cracking tools or vulnerability assessment software – and need to take measures to isolate those students, control the classroom activity and coordinate with computing services staff to preserve the integrity of the University computer network.

Index terms – information security, education, computer security, computer science education, hacking, information assurance, ethics and computers

I. INTRODUCTION

Bill Clark set down his morning coffee and began perusing the intrusion detection logs from the previous day. As the primary network security administrator at the university, he routinely monitored the incoming network traffic for commonly used hacker tools such as BackOrifice, NetBus or SubSeven. Suddenly he notices an entry that indicates an incoming download of SubSeven. He was startled to see that the download was initiated from a university IP address. He checked the location of the IP address and found it was in an office on the first floor of a dorm on campus. He grabbed his coat and drove over to the dorm. The dorm manager indicated that an abandoned office existed on the first floor and was not used except for the storage of some computer equipment that was installed by one of Bill's computing services workers. "The nice young man said he was installing a wireless network access point and not to disturb the equipment." Looking inside the locked office Bill found a computer with no case and 5 hard drives that clearly had been built from scavenged parts. The keyboard had been disconnected and the monitor turned off, but the PC was clearly running. Bill called the university police to investigate. They quickly found that one of Bill's staff, a student worker and computer science major, had installed the computer on what he knew to be an unused campus IP address. The PC contained a variety of hacking tools designed to sniff the network traffic and was hosting an email server that was used by at least 300 other hackers to trade music and information. When the police questioned the student he immediately confessed but insisted he didn't know using the IP address and the hacking tools was illegal. As he stated to the investigating officer," I was just trying to learn Linux better. I didn't mean to cause a problem."

Is there a connection between university computer science (CS) students and the increased malware activity directed against university computer resources? As the above scenario would suggest, students in CS courses are often uniquely positioned to experiment successfully with their knowledge against campus systems. Students know that detection is virtually impossible with so many decentralized systems, that there is weak security, and that their skill sets are often superior to low-paid university staff. Further, students may not

Patricia Logan, Ph. D. is an associate professor in the College of Information Technology and Engineering at Marshall University, Huntington, WV. She teaches information security and computer forensics courses. Allen Clarkson is a graduate student in Technology Management at Marshall University. He has 10 years of experience in network design and management and holds the MCSE certification.

understand the ethical and legal implications of their experimentation.

A review of U.S. v Morris (1991) [1] is instructive concerning the level of experimentation (and damage) that an unsupervised CS graduate student can achieve. The defendant claimed to have released a software worm onto the nascent Internet in order to demonstrate security inadequacies. A CS undergraduate at University of Texas, Austin (2003), apparently also was testing his skills using campus resources to gather data from poorly secured campus servers.[2] This student told officials that he did not intend to use the data to harm anyone.[3] Not much worry has been expressed by teachers or university computer staff despite a number of legal cases with computer science majors indulging their newly acquired skill sets to do mischief. As more universities move into information security and forensics courses (50 schools have qualified as National Security Administration (NSA) Centers of Academic Excellence in Information Assurance (CAE))[4], will we see increased numbers of students who are skilled and able to manipulate the weak university security environment to experiment with their network attack and virus writing skills? With the rise in number of information security courses including computer and network forensics, there is an increased likelihood that the content of these courses will be misused as teachers accelerate the learning curve for students by providing direct instruction in attack tool sets using university labs and computing resources.

This paper deals with the practical issues in implementing a course or emphasis in information security and computer forensics and some philosophical issues that should be considered when reviewing the curriculum. It discusses five areas of exposure for universities and CS departments that can result from students learning to hack, write malicious code, or use forensic tool sets. These areas are:

1. Appropriate hands-on course content for security and forensics classes
2. The role of computing services in the design and use of security labs
3. Student access to courses and majors in security and forensics
4. Computer Science student qualifications
5. University reaction to student attacks

II. Appropriate Hands-On Course Content for Security and Forensics Classes

Few universities have undergraduate or graduate majors in security and fewer offer courses in network or computer forensics. Using the published list of NSA CAEs that require courses in security-related topics, there are at least 50 U.S. universities that have these courses and offer a major. Implementing these courses often means approval by university curriculum committees with reassurances that the content would not be dangerous or present a risk to university computing. At that level, questions are seldom raised about the hands-on exercises or lab facilities. It can be argued that hacking tools, methods, and other types of security course content are readily available on the Internet; a Google™ search reveals hacker web sites and tool sets with instructions and chat rooms for personal assistance. CS departments, however, should be considerably more structured in their presentation of the information and aware of the possibility for misuse or abuse of university resources.

Allowing these courses only at the graduate level possibly ensures that students are more mature, gainfully employed, and therefore, less likely to use course content for malicious experimentation. These assumptions are not supported by the history of on-campus hacking cases which involve both undergraduate and graduate students Some universities avoid the issue altogether by not teaching hands-on content or having separate labs away from general student access to practice their skills. Book and lecture-based instruction is not always as effective in demonstrating concepts as hands-on experience. Separate labs help reduce malicious activity initiated from within their confines, but that solution alone does nothing to protect the wider network from experimentation on other nodes. A question remains about the legitimacy of teaching students to hack in order to improve their detection skills. The same question was asked last year when the University of Calgary announced plans to offer a virus writing course with the stated goal of improving the understanding of virus mechanisms. Opponents argue that formal instruction in writing viruses only encourages more illegal activity. Dr. Ken Barker, chair of the Department of Computer Sciences at the university, contends that "most computer-science graduates today already have the technical knowledge to create a virus" and that the focus of the course is understanding and prevention.[5]

How should students be taught to implement network and desktop security? Is hacking and virus writing a

pre-requisite for developing strong technical skills in detecting malicious activity? What course content should be off-limits? Should courses follow the content for CISSP certification or SANs technical seminars for GIAC certification? Does it necessarily follow that this content, which is appropriate for employed network administrators, is also appropriate for college students?

Faculty have not always discussed the impact of their course content on the security of department and university services. While faculty should be allowed to offer a course that is relevant and provides the skills necessary to be qualified as a security specialist, a discussion with campus computing services should be part of any preparation for teaching these courses. Seldom are faculty privy to the design and security features of a complex campus network. It is reasonable to assume that faculty may propose or require exercises and activities that place the university at risk.

Summary: CS departments need to be practicing, considering, and justifying the methods used to train students in this area. Faculty activities should be described to computing services in advance of course offerings to make sure that they are aware of the potential impacts to the campus network and that procedures are in place to monitor the activity. Adjunct faculty need to be made aware of course content limitations. In the author's experience, adjuncts with strong industry experience are often hired to teach advanced network courses with the result that assignments are often given to students that can compromise a university network. The creation and delivery of courses should consider both the educational needs of the students enrolled and the integrity of the campus network.

III. The Role of Computing Services in the Design and Use of Security Labs

University CS departments often depend on university computing services to maintain labs and install software. What happens when security and forensics courses require installation of tools that if connected to a university network would potentially do damage and violate computer law? Where computer science departments use a general purpose university lab for computer science students, who protects against the improper use of the tools? Should departments assume the risk and configure and manage labs for high security to prevent potential rogue activity? What happens when universities, such as Marshall University, West Virginia house the state's digital evidence lab for the state police, as well as student computer forensic training labs? If computing services require additional tools to effectively manage these unique labs, who will pay for them if they are not part of an existing effort to manage security?

Answers to these questions require a coordinated effort between CS departments and those who are ultimately responsible for the university systems as a whole. As discussed above, computing services departments have a better understanding of the technical relationships among student labs, administrative databases, university data services, email, and the systems and controls that link them all together. In part, computing services can offer expertise in isolating CS students in these courses, but also they can help identify potential flaws in curriculum design that can lead to security breaches. David Dittrich, senior security engineer at the University of Washington, pointed out in 2002 that academic networks are "tempting targets for hackers because of their lack of security, abundance of bandwidth and overworked administrators."[6]

Summary: Though the focus on security has increased in the mainstream press in the past two years, issues of academic freedom tend to leave university networks more open than their corporate counterparts. Including computing services in the design of security labs and curriculum can prevent complicating security further by stemming one potential source of intrusion.

IV. Student Access to Courses and Majors in Security and Forensics

CS students do not often take courses in ethics and law, which are more usually offered in social sciences (criminal justice) or business curriculum. Students are not often taught the law with respect to computing and electronic transmission. A survey of a graduate computer security class at Marshall University found that no students had read the university's Acceptable Use Policies (AUP). Most students are surprised to find that there are laws against copying MP3 files and unapproved wireless access to networks on campus. Each year at least one instructor in a CS course can give an example of students that have managed to find their way into the instructor's network drive, WebCT or other network services that compromise grading or tests. Given the ethical lapses of Enron and Anderson, it appears that

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

business schools were doing an inadequate job of describing to MBA students ethics and the law that resulted in flagrant violations. Universities should never assume that students learn ethical behavior, the laws on illegal network/computer access, outside (or before) their time at the university.

In order to determine whether universities were requiring their CS students to take a course in ethics and computer law, we reviewed computer science major requirements from the websites of the 50 institutions listed on the NSA website as CAEs. These schools were chosen as a representative sample of those that place a high priority on security study. The statistics represented in Figure 1 ***do not*** reflect a study of the CAE programs or course offerings, but instead they represent CS programs at the same institutions. No inference should be drawn from this study regarding the individual CAEs. The integration of the CAE varies widely – some integrate directly into student CS curricula, while others are purely research centers, and still others offer their own academic programs entirely separate from the CS tracks.

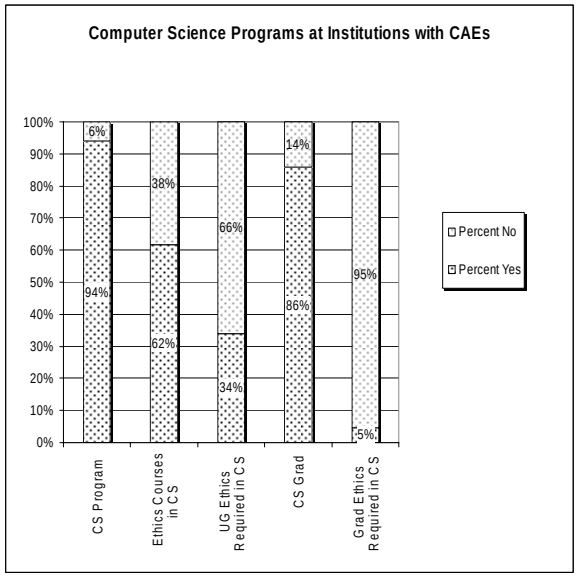

Figure 1

The statistics show that while a solid majority (62%) have ethics courses in their CS program, an even larger percentage (66%) do not *require* undergraduate students to study ethical and/or legal issues as part of a degree program (includes both those institutions that do and do not *offer* ethics or legal issues courses). Further, 95% of all such institutions with graduate studies programs do not require ethics courses. These same universities often have international students that may be unfamiliar with the legal restrictions on computing activities in the United States. It is evident from these percentages that formal instruction in ethical and/or legal issues of computing is not a universal priority in CS curricula even in those institutions with a focus on security.

Could it be that we are training both the "good guys" – security professionals – and the "bad guys" – those with knowledge of techniques and tools but without exposure to ethical and legal issues – at the university level? The statistics from this study show that there may be a disconnect between the study of security and the translation of lessons learned to the rest of the computer-oriented curriculum. Reviewing the CAE schools, the pattern for offering these courses becomes clear: strong technical content and the absence of an ethics and computer law course. Many offer a single course in ethics and law as an elective. What student in this area would by-pass a technical course in order to take a course in ethics? It is apparent that instructors continue to believe that a casual warning about legal/university consequences in a syllabus or brief comment about ethics in an introductory course will be sufficient warning against rogue activity.

Summary: As the role of information technology continues to increase in importance to business and critical infrastructures, additional consideration needs to be given to ethics awareness. Other professions, such as medicine, pharmacology and civil engineering, require that students be exposed to ethical and legal issues in their respective fields. Computer-oriented curricula need to include the same focus for those who will be operating modern infrastructure.

What should we teach in a course on ethics and law? Possible topics include: Cases from the CCIPS web site on FBI investigations and convictions of cybercriminals, which includes some virus writers and improper access (most recently by Adrian Lamo); a review of investigative processes and the specifics of the laws on monitoring, search and seizure, and illegal access of protected data; ethical duties owed to employers and for those who are in the field of computing the ACM code of ethics.

V. COMPUTER SCIENCE STUDENT QUALIFICATIONS

In the last two years, the University of Kansas, University of Georgia, Georgia Tech, Wayne State

University, Columbia University, Indiana University at Bloomington, the University of Missouri, and the University of Texas at Austin, experienced intrusions serious enough that the FBI was called to investigate. No universities publish an updated list of the number of intrusions and outcomes, leaving a question as to how prevalent these activities are, and whether there has been an increase. Dittrich believes that universities are an "especially fertile ground" for student activity and spends a large portion of his time discovering covert MP3 servers and repositories of bootlegged software, music, and movies. [7]

A recent article asserted a correlation between the appearance of malware and student breaks.[8] Can the content of courses lure students into criminal or malicious behavior? Are students with knowledge of campus systems a special case of insider attack? The implication of the article was that students were using break times to practice the skills learned in classes. Is the rise in malware due to efforts of students to improve their skills outside of class assignments? Universities have long been a prime target of hackers, given the open access required by the mission of the university, poorly administered network services, the presence of poorly managed departmental servers, and availability of useful information in unprotected databases.

Summary: Is there a way to detect potential misuse that can become a screening of students as unsuitable to learn computer science? Many majors, such as nursing and the police academy require a separate examination of a student's psychological and personal fitness in order to pursue these fields. Many fields require state-issued licenses in order to practice and require background checks prior to a student's admission into a program. In the same way as these other professional programs screen for suitability, perhaps security and forensics should require not only a high GPA or score on the GRE, but also interviews, and clean criminal records. Should students be screened prior to enrollment in a security program? Should computer science require a professional certification similar to engineering's PE (Professional Engineer) designation? To an extent, this is beyond the purview of CS departments and can only be answered in the longer term by private employment practices and industry developments toward accepted standards and licensure; however, as information technology continues to become less about the technical aspects, and more about the value of the information, CS departments need to consider the roles for which they are preparing their students.

VI. UNIVERSITY REACTION TO STUDENT ATTACKS

Universities have crafted AUPs to respond to the necessity of maintaining and securing computing facilities. How do universities enforce AUPs? Many have banners at logon that students quickly bypass reading. Many students do not see simply "looking" at protected data as unethical. Universities have seldom prosecuted students involved in malicious or unethical use of campus networks. The few cases prosecuted for the illegal use of computing facilities were done by law enforcement not universities. The scenario at the beginning of this article has an ending that is typical of what happens: the student's rogue PC was confiscated, the case was referred to the local law enforcement (no prosecution), and the student was required to "sit out" for one year.

In the absence of strong security and an awareness of the need for creating monitored accounts, should a university worry about downstream liability? Can a university be held responsible for a student's malicious efforts aimed at a corporation or business? A principle tool in protecting the university is the AUP, but it can be most effective only when introduced to students *before* a violation occurs, as a preventative measure, rather than after the fact as a justification for prosecution. Students need to be made aware of AUPs as a regular practice in CS courses. It seems contradictory to give students tools and knowledge that may damage the university system, not explaining the necessary restrictions on their use, and then punishing students for violations. Many universities have specific AUPs for the use of individual sub-networks such as residence halls or libraries.

Summary: As mentioned above, most students are unaware of the university acceptable use policies and any restrictions they might impose. Students in security courses may need accounts that work only under monitoring, signed statements of an understanding of their responsibilities in learning security material, and actual dismissal if involved in misuse. CS departments should consider creating course-level AUPs to augment the university's general use policies that clearly delineate what is being explored for instructional purposes and what is expected of students in their extra-curricular application of the knowledge.

VII. CONCLUSION

University CS departments are moving into information assurance courses at both graduate and undergraduate levels with the current popularity of the major magnified by the large number of job opportunities available in security, access to large amounts of federal funding (NSF scholarship for service or instructional enhancement), and increased focus on the issues by society at large. Students will be trained to use tools and investigative procedures that provide knowledge of hacking and avoidance of detection. The university should recognize this potential risk and work with CS departments to make sure that these students do not practice skills outside of class. Ethics and legal issues need to be included in the study of techniques and tools. Recommendations include: designing a security/forensic lab and curriculum in cooperation with computing services; providing boiler plate language in course syllabi that warns students of violations of university AUPs and the law; requiring students to take a course in ethics and computer law; student accounts that can be monitored and screening CS enrollees in courses that present security/forensic material. Above all, CS departments need to consider the changing role of their subject matter inside and outside of the university. Preparing students to be productive goes beyond providing them with the knowledge; it extends into providing a framework in which to view and use their skills.

REFERENCES

[1] (928 F.2d 504)

[2] http://www.securityfocus.com/news/3174 last accessed February 25, 2004.

[3] http://www.cnn.com/2003/TECH/internet/03/14/university.hacked.ap/ last accessed February 25, 2004.

[4] http://www.nsa.gov/ia/academia/caemap.cfm?MenuID=10.1.1.2 last accessed February 25, 2004.

[5] http://www.pcworld.com/resource/printable/article/0,aid,110938,00.asp last accessed February 25, 2004.

[6] http://news.com.com/2102-1001_3-898084.html?tag=st_util_print last accessed February 25, 2004.

[7] Ibid

[8] http://www.infoworld.com/article/04/01/23/04secadvise_1.html last accessed February 25, 2004