Computer Abuse, Information Technologies and Judicial Affairs

Elizabeth Mackenzie
University of Delaware
Information Technologies
192 South Chapel St.
Newark, DE 19716
(302) 831-1975
betsy@udel.edu

Kathryn Goldman
University of Delaware
Dean of Students Office
218 Hullihen Hall
Newark, DE 19716
(302) 831-2116
kgoldman@udel.edu

ABSTRACT
Crime on the Internet has become a formidable challenge for university information technology and student judicial systems. The nature of university computing requires a relatively unrestricted network, which exposes the university to online hacking, harassment, spam, copyright violations and other computing abuses. This paper will discuss the University of Delaware's efforts to control and prevent online crime while maintaining the open network access required for teaching, research and collaboration by faculty and students.

Information Technologies and the Dean of Students Office at the University of Delaware have worked together to implement policies and procedures to educate students, discourage computer abuse, fairly adjudicate offenders and protect victims. We will discuss these policies and standard practices and our proactive approach to anticipating future threats to computer security.

Next, we will discuss several types of computer abuse typically seen in a university setting. We then outline both the University's response to particular incidents and its efforts toward long-term solutions for each type of computer abuse.

The intended audience for this paper includes both professionals in information technologies, system security and those involved in student judicial systems.

SIGUCCS '00, Oct. 29-Nov. 1, 2000, Richmond, VA.

Keywords
Computer security, computer crime, student judicial system, copyright, Napster, hacking.

1. INTRODUCTION
Computer abuse is a growing problem facing university information technology and student judicial systems. A survey taken at the University of Delaware in fall 1999[1] showed 86% of students own a computer. The opportunity for computer abuse has increased as has the number of cases handled by the Dean of Students Office. There was one case referred to the judicial system in 1996-97, nine cases in 97-98 and eight cases in 98-99. This past year, the caseload included 37 violations of the "Responsible Computing" policy.

Network computing at a university has several properties that make it vulnerable to abuse: 1) a large number of user accounts (the University of Delaware has over 30,000) that presents access and password problems; 2) lack of firewalls and other security tools. A university must allow nearly all network traffic through to accommodate the varied research and teaching needs of faculty and students. This same freedom provides an opportunity for abuse; 3) decentralized server administration. University networks often include servers that are administered outside of information technologies often by untrained personnel. These servers represent potential security problems.

How can we protect our students and systems in such a vulnerable environment? We have found that good policy, cooperation between Information Technologies and the Dean of Students Office and well-documented, standard practices educate students, discourage computer abuse, fairly adjudicate offenders and protect victims.

2. POLICIES AND PROCEDURES

2.1 Responsible Computing Policy

The University of Delaware recognized the need for an "acceptable use policy" early on. The "Responsible Computing Policy" [2]

(http://www.udel.edu/ecce/policy.approved.html),

approved in May 1992, was one of the first of its kind and has served as a model for many other schools. The following extract is the heart of the policy:

"All members of the University community who use the Universitys computing and information resources must act responsibly. Every user is responsible for the integrity of these resources. All users of University-owned or University-leased computing systems must respect the rights of other computing users, respect the integrity of the physical facilities and controls and respect all pertinent license and contractual agreements. It is the policy of the University of Delaware that all members of its community act in accordance with these responsibilities, relevant laws and contractual obligations and the highest standard of ethics."

The Policy also clearly states that computing accounts are a privilege, not a right. Accounts will be disabled whenever abuse of the system is detected.

The Policy is general so that it does not require frequent modifications to accommodate new technologies, yet specific enough to address the four basic computer abuses most often seen on campuses: commercial use of university computing resources, harassment, hacking and copyright violation. The Policy and the Code of Conduct in the Official Student Handbook (http://www.udel.edu/stuhb/) [3] prohibit criminal activity.

In addition to the Policy, every student must read the "Student Manual for Responsible Computing" [4]. This pamphlet clearly explains what is and is not allowed on the University network, who owns what, appropriate use of web pages and e-mail and penalties for abuse of the computer system.

The policy and manual provide all students with the information they need to use the University's computing resources responsibly. When students don't act responsibly, these documents help the Dean of Students handle incidents fairly and equitably.

2.2 ECCE

Students must agree to abide by the Policy before they are given an account on the University system. In addition, each student must take the Electronic Community Citizenship Exam (ECCE); (http://www.udel.edu/ecce/instruct.html). This test is administered via the web. It is composed of 10 questions randomly drawn from a bank of 40. The student must answer every question correctly before he or she is granted access to his or her account. Students may take the ECCE as many times as required to pass.

The exam serves the following two main purposes:

1) The exam verifies that the student has read and understands the "Policy for Responsible Computing." Nine questions on the ECCE are randomly chosen, one question appears on every test; (True or False, "I have read and understand Responsible Computing A Student Handbook including the Policy for Responsible Computing and Recommended Guidelines for Responsible Computing.") If the student answers false, he or she is given a link to the Student Responsible Computing Handbook and the test terminates.

2) The ECCE promulgates University policy regarding rapidly changing technology. While the Policy is a long-term, fairly static document, the questions in the ECCE are changed often to reflect changes in computer technology. For instance, new questions were recently added to address technologies such as MP3s and Napster. These terms did not exist when the Policy was written.

2.3 Student Incidents, Procedures and Reference ("The Blue Book")

In 1999, the Director of System Security and Access and the Associate Dean of Students formalized a process for charging students in violation of the Policy. Formerly, cases were handled individually. This made it difficult to ensure that students committing the same violation were treated equally and fairly.

The result of this formalization is a set of procedures used to report, charge and adjudicate computer violations committed by students. The set of policies has affectionately become known as the "Blue Book."

When System Security becomes aware of a violation, the Director evaluates the abuse and assigns it to one of three levels outlined in the Blue Book. If a serious crime has been committed, the police are notified immediately.

In a recent case, University police obtained a search warrant to require Hotmail to provide a user identity. The user's computer was then confiscated. The student was expelled after being charged with 18 counts of sexual harassment. (Actually, the Responsible Computing Policy did not apply because he conducted this harassment toward another student from his parents' home and did not use any University computing resources.)

Low level incidents include sending chain mail and electronic pyramid schemes. These offenses do not typically require the involvement of the Dean of Students. They are addressed with education and a warning letter. Multiple low level violations will result in a middle-or-high level offense sanction.

Middle level offenses are more serious and include abuse of class mailing lists, spam and copyright violation.

High level violations are the most serious. They include forged mail, illegal FTP sites or name servers, sniffing the network, port scans, denial of service and other types of attacks against computers.

The Director of System Security and Access refers all middle or high-level offenses to the Associate Dean of Students. The referral includes the level of the incident, the student's name, a description of the offense, details and references. The information in this referral is available to the charged party. The computer account of the charged party is disabled until the matter is resolved.

The Associate Dean of Students Office sends a letter to the student explaining the charge(s) and asks the student to attend a pre-hearing. At the pre-hearing, the student can plead guilty or not guilty. If the student pleads guilty or does not attend the pre-hearing, the matter is handled administratively and a sanction may be imposed without further input from the student.

If the student pleads not guilty, a hearing is held. Members present at the hearing include the charging party (usually from IT), the charged party and a hearing officer (a member of the University's professional staff). The student may also invite an advocate to advise him or her during the hearing. This advocate is typically a faculty member or other University professional.

During the hearing, the charging party explains the incident, displays forensic evidence and may call witnesses. Next, the student responds to the charges calling witnesses if necessary. Both the charging party and the student are given an opportunity to ask questions. Each party makes a final statement.

The hearing officer has three days to render a decision. If the student is found not guilty, all references to the incident are deleted from the student's record. If the student is found guilty, the officer will impose a sanction. The student has an opportunity to appeal if found guilty.

Sanctions vary with the type and extent of abuse and are imposed at the discretion of the hearing officer, but sanctions must be consistent. If one student is found guilty of launching a denial of service attack and is sanctioned with deferred suspension, then any other student found guilty of the same offense must be sanctioned the same way unless there are extenuating circumstances. These sanctions are in addition to any sanctions imposed by criminal or civil courts.

In general, middle-level offenses are sanctioned with loss of computing privileges and deferred suspension from the University for one year. This means that if the student is found guilty of any violation of the "Code of Conduct" during the period of one year, he or she will be immediately suspended from the University and banned from the property. High-level offenses are sanctioned with permanent loss of computer privileges, deferred suspension or suspension.

3. TOP FOUR COMPUTER ABUSES ON CAMPUS

The four most common computer abuses seen on this campus are commercial activity conducted on University computers, electronic harassment, hacking and copyright violation. The following sections will discuss UD's experiences and policies for each.

3.1 Commercial Activity

One of the most common computer abuses on campus involves some variant of commercial activity. This commonly includes advertising on web pages and spamming.

The following is an account of the first case handled with the Blue Book. In the fall of 2000, a student was charged with "spamming"-- mass mailing unsolicited or "junk mail" messages. The student was advertising a commercial site on the Internet. The site paid him a commission for each referral generated by his spam.

This case was particularly interesting for two reasons; 1) the site the student was advertising appeared to contain child pornography and 2) a faculty member became an advocate for the student.

The spam went out to over 1,000 users. The subject line contained an offensive description of material on the site. A recipient of one of the message forwarded it to System Security and Access because of the suspicious subject line. The recipient identified the University of Delaware by the IP address included in the message header. The University police were called in, but by the time they investigated the site, it had been taken off-line.

The student was charged with using University computing resources for private commercial activity. The student's defense was that he did not send the spam from his University account; rather he used another mail service. In fact, his university e-mail address did not appear in the message.

While policies are often maligned as unread, dusty documents, the Policy is exactly what defeated this defense. The "Student Handbook for Responsible Computing" clearly defines University computing resources as "the network, all the wires, cables and routers that connect the central computers." The Policy prohibits the use of University computing resources for commercial activity. So, even though the student did not use his University account to send the spam, since he sent the spam from his

dorm room, he used the campus network and violated the Policy.

The student was found guilty and suspended from the University for one year.

The student appealed the decision and, with the advocacy of a faculty member, his sanction was reduced to one semester of suspension. The faculty member argued that the Policy is wrong and should not prohibit any kind of use of the network. She argued for free speech, privacy and freedom on the Internet.

The line between freedom of speech and protection of users on the Internet is being drawn freehand on campuses all over the country. Until the courts decide, universities must rely on their own policies to strike the proper balance.

In response to this and similar incidents, UD Network and System Services (NSS) customized the University's mail server to limit the number of recipients listed on a mail message.

3.2 Harassment

The majority of cases referred to the Dean of Students Office for violation of the "Responsible Computing Policy" involve harassment and are often forged by the sender.

It is not difficult to forge an e-mail address, but the forgery can often be traced back to the internet protocol (IP) address from which the message was sent. On a University campus, an IP address usually corresponds to a specific dorm room.

One case involved forged e-mail containing abusive remarks. The message was traced to a dorm room. Each dorm room has two Ethernet ports. Each port is assigned to a roommate; further, students register the media access control (MAC) address of their computer. This associates a student's personal computer with one of the ports in the room. This kind of forensic evidence is extremely convincing.

The Internet provides a sense of anonymity. This may cause a student to do something he or she would not normally do. Indeed many students faced with charges of harassment claim they were "just fooling around." Students often act impulsively. The more education we can provide about electronic harassment and e-mail abuse, the better our chances are of keeping students out of trouble.

Class mailing lists are often abused causing a "mail storm." Class mailing lists provide a convenient way for instructors to communicate with their class but can quickly get out of control.

In one case, a student sent a chain letter to a class list. The chain letter promised payment for forwarding the message. A member of the class list forwarded the message to mailing lists of all her other classes. Next a student forwarded the message to hundreds of class lists (guessing most using the naming convention for class lists).

Meanwhile, students responded to the message asking the sender to stop. By inadvertently hitting reply-to-all instead of reply to sender, these messages intensified the storm. Many of these responses contained angry and obscene messages. This caused the storm to increase in volume and hostility. By the second day, millions of messages were being transmitted slowly bringing the server to a crawl.

System Security and Access responded by contacting instructors (by phone) and asking them to talk to their classes about the mail storm. The instructors asked students not to respond to the messages, to cease or limit their use of class lists and to be careful with the reply-to-all command.

Several students were charged with abuse of class lists. Thousands of students were involved in the storm, so it was difficult to identify the students who had originated and exacerbated the storm. When the storm subsided, the messages were reviewed. Five students were identified that had added hundreds of class lists to the CC field. These students were the only ones charged.

The cases were covered in the student newspaper. Several stories ran explaining the cause of the mail storm and the money- making scam the message advertised. These articles provided valuable information to the University community.

NSS has since changed the mail system to require that class lists be added in the BCC field instead of the CC field. Since mail storms typically happen in the beginning of the fall semester, IT is considering posting a message in the school paper during the first week of school explaining and warning students about chain letters and pyramid schemes.

3.3 Hacking

Hacking is considered a very serious offense. If a University of Delaware student is charged with attempting to gain access to a computer he or she not authorized to use or to crash a system, he or she will immediately lose their computing privileges and will most likely be suspended from the University. If the student is found guilty of violating US Law (shown below), he or she may face fines and or imprisonment.

US Code Title 18 – Crimes and Criminal Procedure part I Crimes Chapter 121 - Stored Wire And Electronic Communications And Transactional Records Access [5]

Sec. 2701. Unlawful access to stored communications

(a) Offense. - Except as provided in subsection (c) of this section whoever - (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally

exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

Some students, particularly computer science and engineering majors, with newly discovered skills attempt to break into the University's servers. These attempts are usually discovered immediately and reported.

This happens occasionally but more often University accounts are stolen and used as "lily pads" for hackers to launch further attacks. Accounts are stolen largely due to weak passwords.

The University is taking several steps to protect against these attacks. Recently, NSS installed a new password filter (cracklib) to make choosing a bad password more difficult. Currently user passwords never expire, so many bad passwords still exist.

NSS is in the process of advertising a University-wide password change mandate. After informing the University community, passwords will begin to expire. The oldest passwords will expire first followed by newer and newer passwords until all of the passwords have been refreshed. Expiring all passwords at once could cause a denial of service and overwhelm the help center.

3.4 Copyright Violation

Copyright violation is a huge issue on campuses today. It forces administrators to confront difficult issues like freedom of speech, intellectual freedom, intellectual property rights and copyright law.

In some ways this issue is easier for corporations. For profit businesses can bolt down their systems and prevent unauthorized access to the Internet. They are still vulnerable to attack, but they can block any traffic they don't deem essential to the mission of the company.

Universities, on the other hand, thrive on research, cooperation and collaboration. Their systems must be open to foster the educational and creative work of students and faculty and so are vulnerable to abuse.

Napster is a program that allows users to share music, stored in a compressed form called MP3, over the Internet. The program maintains a database of songs stored on computers all over the world. The default installation of Napster scans the user's hard drive for MP3 files. These files are added to the master database. When a user requests a song, they are presented with a list of sites that have the song. Simply click and the file is copied to your computer. Gnutella, is a similar file-sharing client that uses a distributed system rather than a master database.

Napster programs like it are often used to share copyrighted work. According to the Recording Industry Association of America (RIAA), "when you put a sound file containing a recording on your web site, FTP site, e-mail it to a friend, send it through a chat service or send it out by other means, it constitutes a distribution of that sound recording which you need permission to do." [6]

Or more formally, the US law (US Code Title 17 Chapter 11 Sec. 1101 - unauthorized fixation and trafficking in sound recordings and music videos [7]) states

(a) Unauthorized Acts. - Anyone who, without the consent of the performer or performers involved - (1) fixes the sounds or sounds and images of a live musical performance in a copy or phonorecord, or reproduces copies or phonorecords of such a performance from an unauthorized fixation,

(2) transmits or otherwise communicates to the public the sounds or sounds and images of a live musical performance, or

(3) distributes or offers to distribute, sells or offers to sell, rents or offers to rent, or traffics in any copy or phonorecord fixed as described in paragraph (1), regardless of whether the fixations occurred in the United States, shall be subject to the remedies provided in sections 502 through 505, to the same extent as an infringer of copyright.

On the other hand, many network administrators argue that they are not the police. They have to maintain a system where researchers can share high-tech equipment over the network, collaborators can hold a meeting without travel and users have high speed access to all of the resources on the World Wide Web. How can this kind of shared environment be provided while preventing copyright-violating file sharing?

One alternative is to actively search for copyrighted works on systems with Napster. At a university the size of Delaware, this process is logistically impossible as well as a sticky privacy issue.

The remaining alternative is education. Universities have an obligation to protect students from themselves; to tell the students what is and is not legal. Napster is involved in several legal suits [8] that will likely determine the future of music distribution, but in the meantime, the current law is very clear. Anyone who distributes copyrighted material without permission is committing a crime.

Third party liability is another issue currently being debated in court. Depending on the outcome of these cases, universities may be found liable for copyright violations that occur on their networks.

Some universities have decided to block Napster traffic entirely [9]. The University of Delaware has decided

against blocking Napster for several reasons. While Napster can be used to distribute copyrighted material, it can also be used to provide exposure to small bands who have granted users permission to share their music. Blocking Napster traffic may be difficult because it can be configured to run on any number of ports. Blocking all the ports that Napster could possibly use would effectively shut down the network. The University feels education is a better solution. Its efforts to teach students about copyright are detailed below.

4. UD Fights the Good Fight

Education is key to protecting against computer abuse.

4.1 RA Education

Resident Assistants (RAs) provide support to students in their dorms. RAs should be given the resources they need to educate and assist students. Federal and State law, the University Policy and how RAs can help victims of electronic harassment should be included in every RAs training.

System Security and Access and the Dean of Students Office are developing a "fact sheet" to help RAs identify and report computer abuse. The sheet will also contain information on resources available to assist and protect victims of electronic harassment.

4.2 Secure Computing in an Open Environment

Security of university computing systems is critical. These systems contain student records with highly confidential material. The Family Educational Rights and Privacy Act (FERPA) of 1974 [10] outlines a university's obligation to protect this information. Computing in a networked environment will always involve risks, but there are measures universities can take to minimize this risk.

The EDUCAUSE Task Force on Systems Security is recommending that all campus network and technology leaders find and fix the 10 most common security holes on their campus [11] by adopting the advice and methodology of the SANS Institute [12].

Education of system administrators is very important. The University of Delaware has a loosely formed group of system administrators from all over campus. The group meets monthly and shares information on a newsgroup. The members protect their systems by sharing information with each other and using resources on the web like SANS and CERT.

Distributed servers are a serious security problem on many campuses. Information Technology units can improve security by fostering and supporting groups like this.

4.3 Sanctioning Guidelines are Widely Distributed

Students should be aware that the University takes this type of violation very seriously. The sanctions applied put the students' continued attendance at the University in question. Warning students of the consequences is a deterrent to behavior.

4.4 Student Copyright Education Campaign

In the spring of 2000, a group of professionals was assembled to address the issue of student education on copyright issues. The team included representatives from System Security and Access, Network System and Services, UD Library, User Services and the Dean of Students Office.

The team is charged with educating students on copyright issues. Illegal distribution of MP3s and software piracy are the team's first priorities. Some of the team's plans include the following:

Asking artists who perform at the University Performance Hall to pose for posters and appear on campus radio advocating respect for copyright law.

Introduction of copyright education into the curriculum of the mandatory freshman English class.

Including copyright education as part of New Student Orientation.

Other measures will be implemented as their work continues, but the group agrees that education is the answer.

4.5 A Computing Ethics Seminar

This seminar, in the development stage at the time of this writing, will be required for all Responsible Computing violators. The successful completion of the seminar will allow a user to have their University account re-enabled if it is part of a sanction. The seminar will also be offered as a program to residence halls, student groups and other members of the University community, at their request.

5. CONCLUSION

Computer abuse is a growing problem on campuses today. The future is uncharted. Information Technology and Dean of Students Offices can work together to protect students and the institution while providing a rich and open computing environment.

6. REFERENCES

[1] University of Delaware Student Computer Use Survey, conducted 1999, User Services, Information Technologies.

[2] University of Delaware Policy for Responsible Computing

(http://www.udel.edu/ecce/policy.approved.html), Approved May 1992; Revised 2000.

[3] University of Delaware 2000-2001 Official Student Handbook, 2000 (http://www.udel.edu/stuhb/).

[4] University of Delaware Policy for Responsible Computing – A Student Manual (http://www.udel.edu/ecce/toc.html). Revised 1999.

[5] US Code Title 18 – Crimes and Criminal Procedure Part I Crimes chapter 121 - stored wire and electronic communications and transactional records access Sec. 2701. Unlawful access to stored communications.

[6] Recording Industry Association of America, "Soundbyting A Campaign to Protect Music on the Internet – Copyright & Music 101," RIAA (August 1999).

[7] US Code Title 17 – Copyright Chapter 11 Sound Recordings and Music Videos Sec. 1101 – Unauthorized fixation and trafficking in sound recordings and music videos

[8] Sean Silverthorne, "Mr. Napster goes to Washington," (http://www.zdnet.com/zdnn/stories/news/0,4586,2601519,00.html). ZDNet News, July 11, 2000.

[9] Richard Shim, "Streaming a Napster solution on Campus," ZDNet News, July 12, 2000. (http://www.zdnet.com/zdnn/stories/news/0,4586,2601846,00.html)

[10] Family Educational Rights & Privacy Act (FERPA) (http://www.ed.gov/offices/OM/ferpa.html)

[11] SANS, "How to eliminate the 10 most critical Internet security threats." Version 1.25, July 12, 2000. (http://www.sans.org/topten.htm)

[12] EDUCAUSE, Announcing the formation of the EDUCAUSE Task Force on System Security, July 12, 2000. (http://www.educause.edu/issues/security.asp)