Information Technology News of the University of California, Davis

IT TIMES

May 1999

http://it.ucdavis.edu/it.times/

New response and reporting team focuses on computer security incidents

BY DOREEN MEYER

The problems and the benefits of interconnected computer resources at UC Davis affect everyone's ability to conduct university business. On the positive side, staff, faculty and students can use computers to access data and communicate electronically — both on and off campus. On the downside, that interconnectivity makes desktop systems as well as department computers subject to potential security problems.

The same types of network connectivity problems are faced by academia, government, law enforcement, and private industry around the world. The need for the ability to handle security incidents is significant enough that the UC Office of the President in late November 1998 issued Electronic Information Security Guidelines advising each campus to develop an incident reporting system. At UC Davis, IT's Distributed Computing Analysis and Support (DCAS) staff had already begun developing such a program in August 1998.

The Incident Response and Reporting project will address security incidents such as virus outbreaks (remember Melissa?), denial of service attacks (attacks on a system that result in interruptions in service), computer account or server host breakins, port scans (looking for systems with well-known vulnerabilities), UC Davis Acceptable Use Policy violations, and copyright infringements.

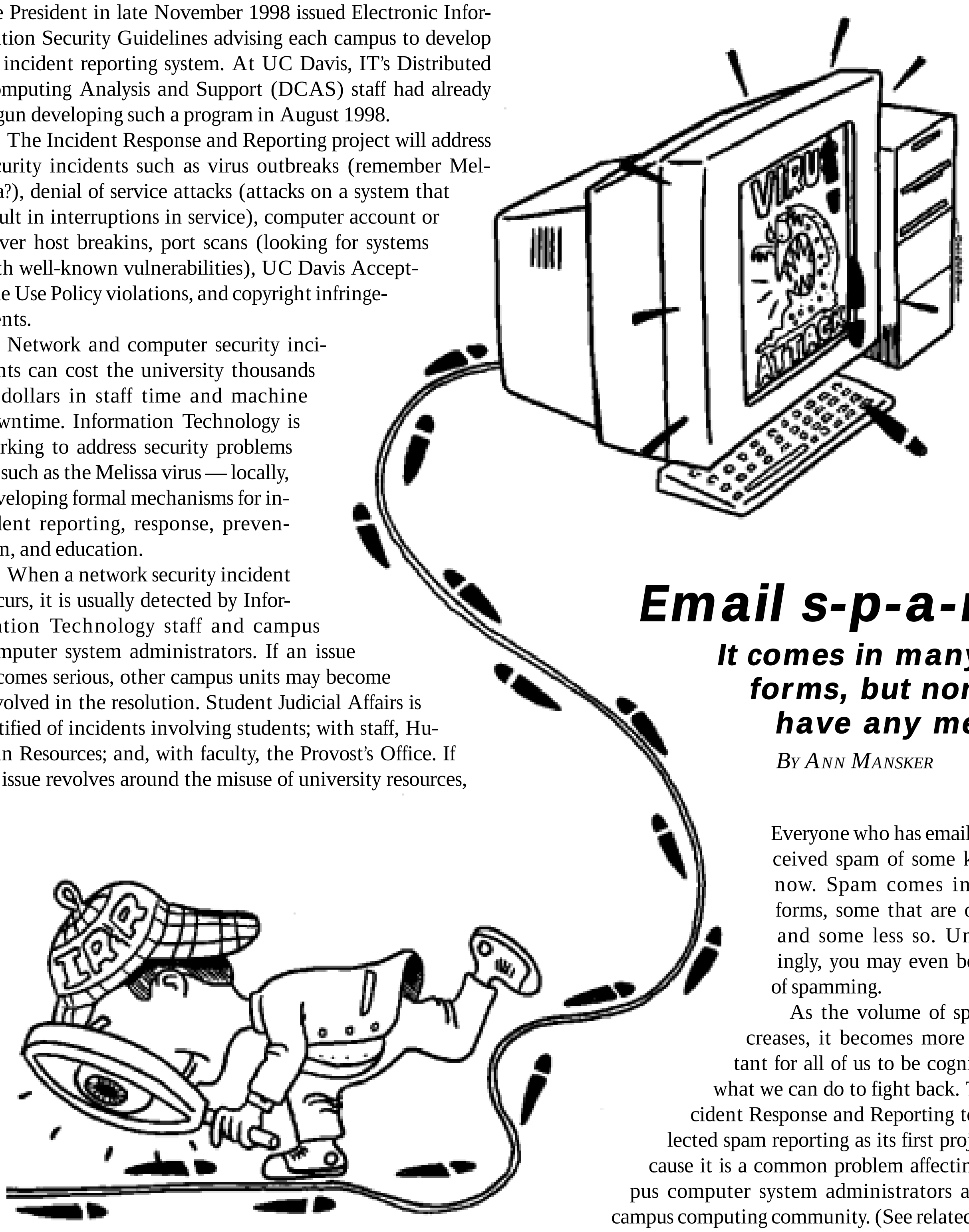
Network and computer security incidents can cost the university thousands of dollars in staff time and machine downtime. Information Technology is working to address security problems — such as the Melissa virus — locally, developing formal mechanisms for incident reporting, response, prevention, and education.

When a network security incident occurs, it is usually detected by Information Technology staff and campus computer system administrators. If an issue becomes serious, other campus units may become involved in the resolution. Student Judicial Affairs is notified of incidents involving students; with staff, Human Resources; and, with faculty, the Provost's Office. If an issue revolves around the misuse of university resources, the Campus Misuse Committee and possibly Internal Audit will be notified. If a security incident is potentially illegal, the Police Department will be alerted.

One of the issues the Incident Response and Reporting team members will discuss and resolve in the next few months is how to avoid duplicating efforts to resolve an incident, wasting time and resources in the process. Duplication of effort can occur, for example, when staff members not in direct commu-

see Incident Response on page 5

IN THIS ISSUE



Email s-p-a-m:

It comes in many forms, but none have any meat

BY ANN MANSKER

Everyone who has email has received spam of some kind by now. Spam comes in many forms, some that are obvious and some less so. Unknowingly, you may even be guilty of spamming.

As the volume of spam increases, it becomes more important for all of us to be cognizant of what we can do to fight back. The Incident Response and Reporting team selected spam reporting as its first project because it is a common problem affecting campus computer system administrators and the campus computing community. (See related article on this page.)

ILLUSTRATION BY STEVE OERDING/IT-CREATIVE COMMUNICATIONS SERVICES

see s-p-a-m on page 2

s-p-a-m: *It's unsolicited*

continued from page 1

What is spam?

Technically, SPAM (tm) is a potted meat product composed of chopped up pork shoulder and ham, invented by Hormel Foods, Inc. in 1937. The word was originally adopted as slang for unsolicited commercial email (UCE). It is now commonly extended to several varieties of email and newsgroup abuse, loosely categorized by using the Internet to deliver inappropriate messages to unwilling recipients. Hormel Foods has posted its admirable position on UCE and the use of the word "spam" on the Web at *http://www.spam.com/ci/ci_in.htm*.

Spam is:

• Unsolicited commercial email (UCE), such as advertisements for goods and services, which may be anything from discount office supplies to XXX-rated adult Web sites. Though some offerings may be more offensive than others, they are all fundamentally the same kind of abuse.

• Chain letters. The most infamous example is any variation on "Make Money Fast!" but there are others that don't involve money. The ones that do are a felony (mail fraud) in addition to being a form of spam.

• Off-topic or otherwise inappropriate posting. This can be either to a mailing list or to a newsgroup, and includes cross-posting messages to numerous unrelated newsgroups and posting many single identical or nearly identical messages to many groups. It is usually, but not always, commercial in nature. An example of this form of spam is posting a message concerning your litter of kittens (free to a good home!) on a mailing list devoted to NT security updates. Another example is posting an incensed reply regarding someone else's litter of kittens to the entire list, rather than to the sender.

Spam isn't:

• Posting to a newsgroup or list messages that castigate the subscribers as <insert blanket insult> for engaging in whatever activity the newsgroup or list is concerning. This is known as "trolling," and exposes the troll as immature and socially backward, but is almost by definition on topic for its target.

• Using email or newsgroup posting to publicly or privately harass another person. Harassment is a violation of the UC Davis Acceptable Use Policy and may result in disciplinary action. In some cases it could even result in arrest and prosecution.

• Forwarding false virus warnings. The "virus" in this case is the warning itself, which is almost invariably a hoax (see *http://www.symantec.com/avcenter/hoax.html* for a list; many will no doubt sound familiar). This is a particularly nasty and insidious thing. It abuses the concern that people have for their friends and co-workers, and uses naïve goodwill to waste network bandwidth.

Illustration by Steve Oerding/IT-Creative Communications Services

Please notice from the examples that spam isn't the only way to abuse campus computing resources. There are lots of other ways, but they happen to be outside the scope of this article.

Are you part of the problem?

If you engage in any of the activities mentioned in what "spam is," you are a "spammer" and may be subject to disciplinary action. No one in the academic community is exempt.

It's also possible to be part of the spam problem without actually generating any mail yourself. If you are responsible for a computer that is on the network and is capable of functioning as a mail server, you could be providing a service to spammers by giving them a conduit to get around the efforts of other administrators to block the unwanted traffic. The service, called "relaying," is enabled by running mail server software configured to accept and forward messages that are neither from nor to a *ucdavis.edu* address. Spammers love to find relay-enabled hosts, especially in a respectable domain such as *ucdavis.edu*, because it lets them spout thousands of messages that would be blocked if they were coming directly from their true source.

> *If you are responsible for a computer that is on the network and is capable of functioning as a mail server, you could be providing a service to spammers by giving them a conduit to get around the efforts of other administrators to block the unwanted traffic…(It's) called "relaying."*

Any system that supports mail transport may have a default configuration allowing mail relaying. It is the responsibility of the system administrator to check the mail transport application configuration. In the past few years, system administrators have become more savvy about setting this configuration properly. According to the Mail Abuse Prevention System, "In February 1998, the Internet Mail Consortium (IMC) released a survey reporting that 55 percent of the Internet mail servers remain vulnerable to unauthorized third party relay. Not too long ago, nearly every mail server was vulnerable to relay. So, although there is a lot of work left to do, we've made remarkable progress over the past few months."

If you have Microsoft Exchange Server, don't feel smug. Relaying was the default configuration for Exchange Server when it first came out. Are you sure you've fixed it? If you are not running server software, you aren't relaying, so all the people using Eudora to download their mail from the central campus POP servers can breathe a sigh of relief.

You're wondering why you should care, aren't you?

The two spam issues that have the most direct impact on the campus are relaying through a campus host, and spam generated at UCD that is directed at least in part to off-campus addresses. Both of these, if unchecked, can lead other sites to block mail from the *ucdavis.edu* domain. This can have very negative effects on you as an innocent end user. Imagine you're submitting an application for a grant that will support your entire lab for three years. Or, imagine you're in the midst of negotiating the summer internship of your dreams with the company you hope will give you a terrific job when you graduate. Or, imagine you've just finished the final corrections on the manuscript that the department chair has assured you will make him world famous, and email it to the journal a healthy two hours before the final deadline. Now imagine that your mail bounces because that site has just blocked delivery from *ucdavis.edu* because of spam originated at, or relayed by, UCD.

If you're not an innocent bystander, direct consequences of spamming could include losing your computing account, having a reprimand in your personnel file, or facing a lawsuit. Being a mail relay is bad for your computer because it diverts CPU and memory from your applications. Since spammers generously share the addresses of relaying systems with each other, the end result can be that your system's resources are overwhelmed by the volume of mail, locking you out entirely or crashing your system.

How to tell if your system is relaying, and what to do if it is

There are online resources available for system administrators who wish to make sure their site is not being used for mail relay. The key links are:

http://dcas.ucdavis.edu/security/tools/relaytest.html — A test you can run against your system to determine if the SMTP (Simple Mail Transport Protocol) service is open to mail relay.

http://maps.vix.com/tsi/ar-fix.html — Assistance with disabling relaying on many different mail programs.

ftp://ftp.ucdavis.edu/sendmail.d/ — If you are using a UNIX system with sendmail as the mail transport agent, pre-made program and configuration files for several versions are available for download. The README file on that page outlines the procedure for using the files.

What to do if you're spammed

First, retaliation is a bad idea. Deliberate spammers often forge the return address on the message to deflect retaliation efforts, so you may end up punishing the wrong person. In addition, some forms of payback are themselves grounds for disciplinary action. Last, but certainly not least, replying directly to the spammer (if it is a real address) just confirms that *your* address, at least, is live.

The amount of spam infesting the Internet increases daily. UCD blocks a long list of well-known spam domains, but there are always more where those came from. You have three or four options for dealing with spam that lands in your mailbox:

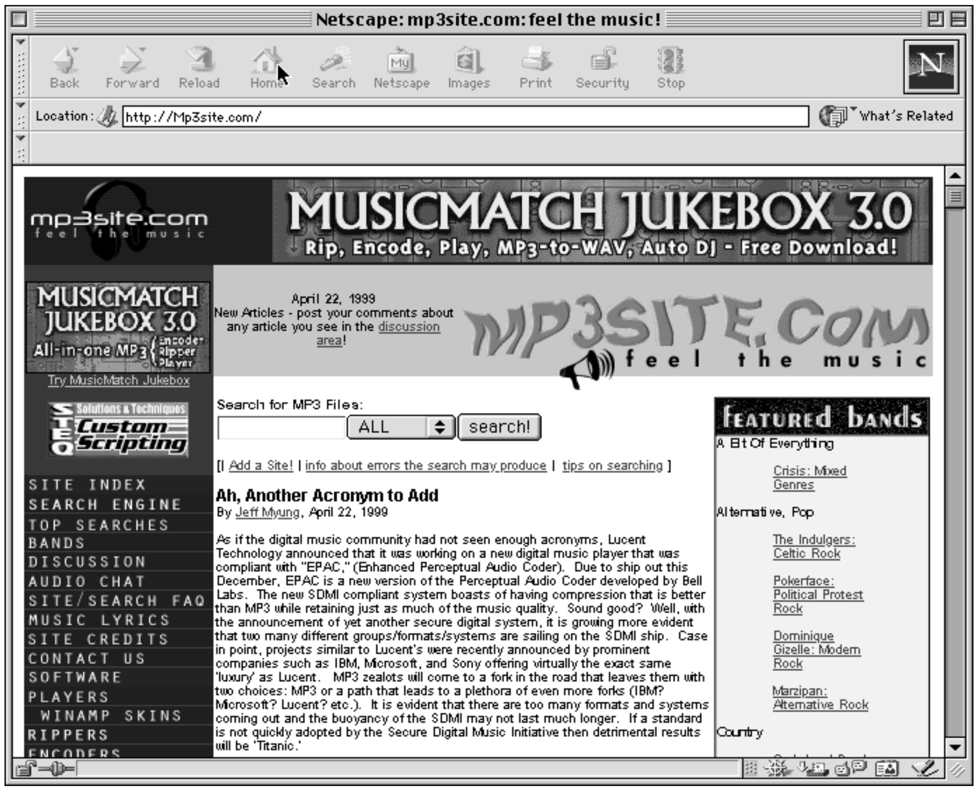
1. Delete and ignore it.
2. Filter it (not readily accomplished by Pine users and can be difficult to set up effec-

see Email on page 7

Now Hear This

Uploaders, Downloaders Need to Mind Their Ps & Qs When It Comes to MP3s

By Matt Peters



April 22, 1999
New Articles - post your comments about any article you see in the discussion area!

[| Add a Site! | info about errors the search may produce | tips on searching]

Ah, Another Acronym to Add
By Jeff Myung, April 22, 1999

As if the digital music community had not seen enough acronyms, Lucent Technology announced that it was working on a new digital music player that was compliant with "EPAC," (Enhanced Perceptual Audio Coder). Due to ship out this December, EPAC is a new version of the Perceptual Audio Coder developed by Bell Labs. The new SDMI compliant system boasts of having compression that is better than MP3 while retaining just as much of the music quality. Sound good? Well, with the announcement of yet another secure digital system, it is growing more evident that two many different groups/formats/systems are sailing on the SDMI ship. Case in point, projects similar to Lucent's were recently announced by prominent companies such as IBM, Microsoft, and Sony offering virtually the exact same 'luxury' as Lucent. MP3 zealots will come to a fork in the road that leaves them with two choices: MP3 or a path that leads to a plethora of even more forks (IBM? Microsoft? Lucent? etc.). It is evident that there are too many formats and systems coming out and the buoyancy of the SDMI may not last much longer. If a standard is not quickly adopted by the Secure Digital Music Initiative then detrimental results will be 'Titanic.'

A Bit Of Everything
Crisis: Mixed Genres
Alternative, Pop
The Indulgers: Celtic Rock
Pokerface: Political Protest Rock
Dominique Gizelle: Modern Rock
Marzipan: Alternative Rock
Country

Mp3site.com is one source of legal MP3s.

What Matt Bradley was doing had a certain sense of 'coolness' to it. It also had a definite sense of illegality.

Last fall, the third-year transfer student moved into a dormitory, giving him access to a ResNet connection. A system administrator for more than two years before attending UC Davis, Bradley was also a music fan, interested in electronic music and composition. Merging his interests in music and computers, he created an MP3 distribution site.

MPEG-2 Layer-3 Audio — or MP3 — is a file format used to store sound digitally. MP3s — the most popular type of music distribution files on the Internet — keep files relatively small, have near-CD quality, and are easily distributed over the Internet.

"Having a fast 24/7 connection was too much of an opportunity to miss, so I decided to put up an MP3 FTP site," says Bradley, who is in the process of shifting his major from physics to computer science and engineering.

"I downloaded a shareware FTP server, registered a domain name... and I was set, not having spent a penny," says Bradley. "I had the site up and running the first week of the fall quarter. I set up the server to allow only a few connections and to limit the bandwidth so I didn't soak it all up and slow down everyone else's connection."

Within days, the number of users and the bandwidth had peaked. Starting with less than 100 MP3s, his site soon had received more than 10,000 'hits,' uploads had swelled his MP3 collection to 500, and a 2 gigabyte hard drive dedicated to the site was full.

> *'I was expecting nothing more than being told to take down my site and a warning to not do it again. I would tell them that I had already taken my site down and everything would be ok. I was wrong.'*
>
> *— Matt Bradley*

"I had my ICQ (chat) number on the site and I received messages from all over the world from people who were using my site," says Bradley. "I communicated with one guy from Russia several times. I thought the fact that people from all over the world were logging in to my computer sitting in my dorm room was very cool."

It was. But again, it also was illegal.

Like many students, Bradley "knew that the legality was a sketchy issue. I was under the impression that as long as the distributor (me) was not making any profit it was legal."

Illegal MP3 sites violate copyright law, according to the Recording Industry Association of America, a nonprofit trade association. "Because the Internet is a new frontier, there is widespread misconception about what is allowable in the context of music and the Internet," reads an RIAA release.

"If you don't hold the copyright to a sound recording, you can't reproduce the work or distribute it...This means that, as a general rule, you can't copy it onto a server, download it, upload it, save it to your hard drive or put it on a disk."

Bradley says his MP3 site was found by someone working for the RIAA, and that the RIAA then informed the UC Davis Division of Information Technology.

"I was reading my email or something one day when all of a sudden I completely lost my Internet connection," says Bradley. "About five minutes later, there was a knock on my door and I got a package hand delivered to me by my RA. It contained a notice saying that my ResNet port had been deactivated because of 'information that raises questions concerning your use of your residence hall ResNet privileges.' It was very vague, but I figured it must have been because of my MP3 site. I figured IT was mad because of the amount of bandwidth I had been using. I didn't think the content of the site was the issue.

"I went back to my room and reconnected to the Internet through dial-up with my modem and unregistered my domain name," says Bradley. "When I went in to meet with (the Student Judicial Affairs officer), I was expecting nothing more than being told to take down my site and a warning to not do it again. I would tell them that I had already taken my site down and everything would be ok. I was wrong."

Donald Dudley, a Student Judicial Affairs officer, says an average of eight to 10 students each year are referred to the Student Judicial Affairs office for distributing MP3s illegally. "The number of referrals has increased with the use of the Web and, of course, with access to a high-speed connection through ResNet," says Dudley.

see MP3s on page 8

Myths about MP3s

If I upload music from a CD that I own, I'm not violating copyright law.
FALSE. Owning a CD doesn't mean you "own the music." You can't put music on the Internet without permission of the copyright owners.

If I don't charge people for downloading music from my site, I'm not violating copyright law.
FALSE. If you don't hold the copyright, you cannot authorize downloads of sound records — even if you don't charge a fee.

If I only download sound recordings, it's not a violation of copyright law.
FALSE. It's a violation if you upload or download copyrighted sound recordings without permission of the copyright owners.

The "fair use" exemption protects me.
FALSE. Some uses may be "fair," but uploading or downloading full-length recordings without permission is not "fair use."

If a Web site doesn't display a copyright notice for the music, the music isn't copyrighted.
FALSE. In the U.S., almost every work created privately and originally after March 1, 1989 is copyrighted and protected whether or not it has a notice.

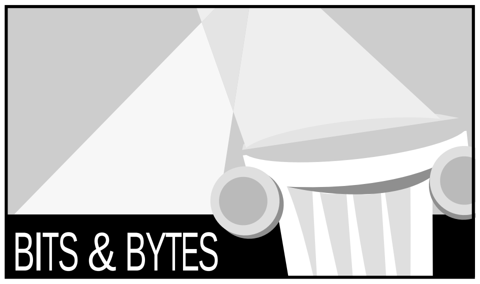
If I upload or download a sound recording and leave it on my drive for less than 24 hours, it is not copyright infringement.
FALSE. Whether you upload or download a sound recording and keep it for 24 hours or 24 seconds, you are still violating copyright law.

An MP3 site is legal with a disclaimer on it.
FALSE. It doesn't matter how many disclaimers you put on an MP3 site. If you operate an MP3 site, you're violating copyright law.

It's within my First Amendment (free speech) rights to create an MP3 site.
FALSE. The First Amendment does not include the right to infringe copyrighted works.

Distribution of music doesn't hurt anybody. It's promotional and free advertising.
FALSE. It's up to the artist and copy-

see Myths on page 8



Three Major Changes Implemented in April

Last month, changes were made to three major campus computing resources: the Staff/Student Modem Pool, the Student Information System, and the UC Davis Financial Information System. Email notifications were sent to all current and potential users in the weeks leading to the changes. If you use any of these resources and are experiencing difficulty accessing them, the following will give you an overview of the changes and identify who you may contact for assistance.

1. Staff/Student Modem Pool

When did the change occur?
Tuesday, April 27.

What is the change?
All campus modem pools are equipped with secure authentication mechanisms. Prior to April 27, the authentication mechanism was not enforced on the Staff/Student Modem Pool. Now, when accessing the modem pool, all staff and students need a new-style LoginID (to access UC Davis computing resources), an IRAS ServiceID (to access the Student/Staff Modem Pool specifically), and a Kerberos password (to authenticate each connection to the network).

Who was affected?
The individuals affected by this change are staff and students who are missing a new-style LoginID, an IRAS ServiceID, or a Kerberos password. All three are now rigidly enforced on the Staff/Student Modem Pool. You were not affected by this change if you:

- already had a new-style LoginID, a Kerberos password, and an IRAS ServiceID prior to April 27.
- always use one of the other modem pools (i.e., the 56K Faculty Modem Pool or the 14.4K Legacy Modem Pool).

What to do if you are experiencing difficulties:
If you are denied access to the Student/Staff Modem Pool, you need to verify that you meet the three requirements listed above. To convert, or to verify that you meet all the requirements, point your Web browser to *http://mothra.ucdavis.edu* or contact IT Express at (530) 754-HELP. IT Express consultants are available in Room 182 Shields Library for assistance with the conversion process.

2. Banner Security Upgrade

When did the change occur?
Saturday, April 17.

What is the change?
Banner's security infrastructure was improved to further protect the confidentiality of student records. (Banner is the UC Davis Student Information System.) Registered users now log in to the system using both a Kerberos password and a one-time password (provided by a hard-token card).

Who was affected?
All registered Banner users (approximately 1,100 individuals). If you are not a registered Banner user, you need not be concerned with this upgrade.

What to do if you are experiencing difficulties:
If you are experiencing difficulties accessing Banner from on campus, visit the Registrar's Web site at *http://registrar.ucdavis.edu/training*. The site provides an overview of the changes made to the log-in process and the steps you need to take to be able to access the system. You should also have received several notifications by email in the weeks preceding the April 17 upgrade.

The individuals affected by (the Staff/Student Modem Pool) change are staff and students who are missing a new-style LoginID, an IRAS ServiceID, or a Kerberos password. All three are now rigidly enforced on the Staff/Student Modem Pool.

If you are experiencing difficulty accessing Banner through the Student/Staff Modem Pool, you need to verify that you have a new-style LoginID, a Kerberos password, and a ServiceID called 'IRAS.' For more information on how to resolve these issues, see "Student/Staff Modem Pool" (#1). Keep in mind that the source of the difficulty might be related to either the new Banner log-in process or the Student/Staff Modem Pool security upgrade.

Questions about the Banner upgrade can be directed to the Banner Help Desk at *BannerHelpDesk@ucdavis.edu* or (530) 757-8996.

3. DaFIS 2.7 Upgrade

When did the change occur?
Saturday and Sunday, April 24-25.

What is the change?
DaFIS is the UC Davis Financial Information System. The most important component of the upcoming change to the DaFIS system was an upgrade to the Oracle database.

The DaFIS system is built on software provided by two vendors: Oracle (for the database), and Compuware's Uniface (for the graphical user interface in transaction processing). To receive continuing support from Oracle and Compuware, it was critical that the DaFIS team upgrade both packages. More specifically, the change entailed upgrading

- Oracle to version 8.05
- the Uniface software to version 7.2.03, and
- the Oracle middleware from SQL*Net client 2.2 to Net8 client 8.04.

The new release includes no new functionality. DaFIS continues to be functional on Windows 95, 98, and NT operating systems.

Who was affected?:
All registered DaFIS users. If you are not a registered DaFIS user, you need not be concerned with this upgrade.

What to do if you are experiencing difficulties:
All DaFIS users have been notified of the upgrade by email through the DaFIS list server. To access DaFIS Transaction Processing, you need to run a special installation script.

Information and instructions on how to prepare for the upgrade are available on the following Web sites:

- DaFIS: *http://accounting.ucdavis.edu/DaFIS/*
- Desktop Systems: *http://desktop.ucdavis.edu* .
- Troubleshooting Web page (for Oracle install errors): *http://desktop.ucdavis.edu/projects/DaFIS/DaFISfix.html*

If you have questions, contact the DaFIS help desk at *dafishelp@ucdavis.edu* or (530) 757-3355.

Campus Directive on Caller ID

A campus directive was issued April 21 announcing upcoming changes to the campus telephone system. The changes that IT-Communications Resources will implement this month are designed to keep the campus telephone system current with the public telephone network. Changes will be made to outgoing and incoming calls placed from a campus phone.

For outgoing calls, you will have the option of blocking Caller ID either on all calls or on a per-call basis. If you block all outgoing calls, you will be able to unblock calls on a call-by-call basis by dialing *82 before composing the destination phone number. If you choose not to block all outgoing calls, you will be able to selectively block calls by dialing *67 before composing the phone number.

The telephone system changes will also expand Caller ID on multi-line sets to include all incoming calls, from on or off campus, that do not have Caller ID blocked. If you have a multi-line set, the caller's telephone number, including area code, will now be displayed on your telephone set (replacing the current "DIDV" code). If the caller has Caller ID blocked, however, the message displayed will be "BLOCKED" or "PRIVATE."

Caller ID changes made by May 7 are free of charge; subsequent changes will cost a reconfiguration service charge of $21 per subscriber line.

To have your telephone number blocked, you need to contact your department's Area Telephone Representative (ATR) by May 7. For further information, please call your Communications Resources Customer Service Representative or the Communications Resources office at 530-752-4603.

To read the campus directive (#99-050), point your Web browser to *http://chancellor.ucdavis.edu* and click on the "UCD Directives" link. A list of frequently asked questions about Caller ID is available on the Web at *http://cr.ucdavis.edu/*.

Campus Directory Updates Needed

IT-Communications Resources is beginning the publication process for the 1999-2000 UC Davis & UCDMC Directory. The directory update packets will be delivered to campus departments starting May 1.

When you receive your packet, please carefully review your department's listings and fill out the directory update forms. Directory Services needs your forms, with your department's most current information and listings, by May 21. Send your updates to "Directory Services, UC Davis."

If you do not receive your packet by May 7, please contact Pat Elkins at (530) 752-8972 or Linda Nixon at(530) 752-8970.

Any Suggestions?

We welcome article suggestions from our readers. Let us know what you would find useful to read in the *IT Times*. Are you using technology in creative and inspiring ways? Have you developed a Web site or other online resource that others should know about? If you have a question related to the use of technology, we'll ask an expert to help.

Send your article suggestions to the editorial team at *itpubs@ucdavis.edu*.

Surge IV: If You Build It, They Will Compute

By Jeffrey van de Pol

Prompted by the success of The Station in the Memorial Union, IT-Information Resources in March opened a third open-access computer facility on campus.

Located in Room 301B of the Surge IV annex (west of the Silo), the new computer "lab" opened its doors the first week of March and was quickly discovered by students.

"The facility opened at 4 p.m., and by Tuesday afternoon the room was already filled and lines were beginning to form," says Peter Blando, operations manager for Lab Management. "Signs were posted at the other computer rooms, and it appears that the word has spread very quickly."

Open-access computer rooms, different from mixed use labs in that the rooms are never reserved for classes, have become an increasingly popular choice among students looking for a quick, reliable method of accessing the campus network while on campus.

The new open access computer room in Surge IV is equipped with 30 computers.

The new computer room is equipped with 18 PC-compatible computers and 12 Macintosh computers, each with a standard package of campus software (including Microsoft Office). The room is open for use seven days a week.

As with The Station, the new computer room is in a convenient location. Situated next to the Silo (a hub of student activity), "The Surge" is close to a parking lot and several Unitrans bus stops, providing the quickest access of any on-campus computing facility.

Space for the new facility was made available through the assistance of the Office of the Registrar and the relocation of IT's Visualization Lab, which allowed Information Technology to come in and prepare the classroom for computer access.

The preparation was no simple task. While a computer room designed for classroom usage already exists next door in 301A Surge IV, extensive renovation of 301B was necessary to make the new space a viable computing workspace.

"A room full of computers and people produces a large amount of heat," says Blando. "Without sufficient ventilation, the area can quickly become uncomfortable. The previous ventilation system, while adequate for the room's original uses, wasn't deemed capable of handling the additional load and was completely renovated. The entire electrical system was also upgraded."

While the new facility is modeled on the success of The Station, recent studies by Lab Management have led to a few changes in the new facility.

The Surge IV computer lab features a higher percentage of PCs, reflecting the higher usage patterns of PCs in other labs. The PC stations are also equipped to read PC formatted ZIP disks, as an increasing number of students need a portable large-file alternative to the standard floppy disk.

Absent are the quick stations which require users to stand while accessing the campus network.

Blando says future expansion plans include a new computer classroom in 1 Olson by the summer, and general consensus is that it will prove as popular as its predecessors.

One can almost hear it in the air on campus: If you build it, they will compute.

Resources:

To check computer room availability, see IR-Lab Management's Web site at: *http://lm.ucdavis.edu/rooms/available/*

To read the latest Lab Management Report (released in Fall 1998) see:: *http://lm.ucdavis.edu/pubs/labrep/fall98/stats/*

Incident Response

continued from page 1

nication are contacted by different sources regarding a potential security incident. By eliminating overlapping effort, the security team can increase its incident response efficiency.

Other issues the team will address are:

- How can team members easily notify the appropriate personnel about a specific problem? For example, if the campus is being scanned for Silicon Graphics vulnerabilities, what needs to be put in place so all SGI system administrators can be contacted immediately?
- How can team members assess the severity of an incident? What criteria need to be present before making a decision to turn off a port that is under attack (thereby shutting off access from that machine to the campus network)?
- How can team members track and record their efforts to resolve an incident and make that information available to other team members and appropriate campus staff?
- Who should the end user or system administrator contact to report a security incident? (Currently, suspected security incidents should be reported to *security@ucdavis.edu*.)

The cornerstone of the Incident Response and Reporting project is Remedy, a trouble ticket system application already in use for other functions in some IT departments. By assigning a unique number to each incident, the trouble ticket system will allow specific individuals in IT to receive and track trouble calls. The program features a reminder that will alert response team members to follow up on a reported incident when a given period of time has elapsed.

> *By assigning a unique number to each incident, the trouble ticket system will allow specific individuals in IT to receive and track trouble calls.*

The team investigating potential problems will be able to view a list of tickets that are pending, and assign themselves the responsibility of following up on the question, and recording their actions when doing so. Other team members will be able to view the tickets, and perhaps gain clues about a security incident from a number of seemingly unrelated ticket submissions. The Web-based Remedy program also will allow UC Davis system users who have filed a complaint to check on the status of their tickets.

With a trouble ticket system in place and a coordinated response by the security staff across organizational boundaries, IT will be able to:

- Provide a point of contact for the campus community for the submission of a suspect security incident.
- Assign a case number and follow up on the submission.
- Minimize the impact of security incidences on a department or end user.

As this program is put into place, the Incident Response and Reporting team will be able to gather statistics on incidents at UC Davis and determine where IT should focus its resources. Initially, the team will be looking specifically at electronic junk mail (see related story on page 1) and later at general network incidents.

Doreen Meyer is a programmer/analyst with IT-Distributed Computing Analysis and Support, and project manager for the Incident Response and Reporting project.

Resources:

For more information on the Incident Response and Reporting project contact Doreen Meyer at *dimeyer@ucdavis.edu*.

To follow IT's progress on incident response, see the project Web site at *http://dcas.ucdavis.edu/security/*.

For a look at national trends, as monitored by the federal incident response network, see *http://www.fedcirc.gov/*.

CENIC '99

Conference will explore application development for Internet 2

CENIC '99

Achieving Critical Mass for Advanced Applications

This year's annual Corporation for Education Network Initiatives in California (CENIC) conference, held May 6-7 in Monterey, focuses on "Achieving Critical Mass for Applications." The conference is open to anyone, including educators, researchers, business persons, and government representatives. Registration information is available on the Web (see Resources below).

Russ Hobby, director of IT-Advanced Networked and Scientific Applications (ANSA) and chairman of a CENIC technical planning group, is looking for comments and suggestions from anyone who is interested in using high bandwidth applications to collaborate with other high-level research institutions. The ANSA director would like to take the information with him to CENIC '99, but says he would welcome such information at any time. Also, contact him if you would like to develop such applications.

The Corporation for Education Network Initiatives in California was formed in January 1998 to develop a high speed, wide area communications infrastructure offering guaranteed, quality service. The formation of CENIC allows its members, representing the state's institutions of higher education, to pool funds and develop a more robust network with higher bandwidth.

CENIC '99's workshop format is designed to further a consensus on the issues involved in middleware and advanced applications, say conference organizers. Hobby describes middleware as the programs which run between the applications and the network, increasing the quality of routine functions.

"One of the things we want to explore is what kind of tool sets can be developed so the applications don't have to be built from the ground up every time," says Hobby. At the conference, Hobby will lead a focus group that will explore why these applications aren't being developed and what's lacking in the current standards for creating such applications.

Conference organizers hope to:

- Develop strategies for optimizing distributed research partnerships.
- Identify suggested areas of collaboration and mechanisms for avoiding duplication of effort.
- Identify research areas where middleware may enable applications with minimal modification to the application.
- Elucidate what middleware can and cannot provide.
- Compile a list of specific research areas which warrant priority funding in order to speed the deployment of advanced applications.
- Draft a proposal for a specific set of advanced application utilities which can be widely and immediately deployed.

A breakout session will discuss opportunities for federal agency grants, which will help application developers get funding for what they want to do, says Hobby.

Notes from the conference will be posted on the CENIC Web site.

Resources:

CENIC: *http://www.cenic.org*

CENIC '99 conference: *http://www.cenic.org/cenic99/index.html*

Russ Hobby: *rdhobby@ucdavis.edu*

Norton's new software: It gets the bugs out

By Leigh Ann Giles

This month, we bring you two products by Symantec Corporation, a provider of utility software for business and personal computing. These products are designed to keep two "evils" at bay, ensuring that your computer remains safe and reliable. What are those creepy evils, you ask? Plainly put: unforgiving viruses and the Millenium Bug.

Norton AntiVirus Agreement

We have finalized an agreement with Symantec for Norton AntiVirus Solution Suite. The decision to acquire 14,000 licenses of this product was based on an evaluation of anti-virus software conducted by the CAIT (Center for Advanced Information Technology). The results of this evaluation will be published in the form of a Recommended Solution document by the end of the month. One of the key features that distinguishes Norton AntiVirus from the other products evaluated is "Live Update." With LiveUpdate, you can keep your anti-virus software up to date by connecting directly to Symantec's Web site and downloading the newest virus definitions. The agreement also provides access to the Norton System Center, which includes administrative tools for deploying Norton AntiVirus across a network.

The products included in the Norton AntiVirus Solution Suite are:

Norton AntiVirus 5.01 for Windows 95/98
Norton AntiVirus 5.01 for Windows NT Workstation and Servers
Norton AntiVirus 5.0 for OS/2
Norton AntiVirus 1.5 for MS Exchange
Norton AntiVirus Plus 5.0 Tivoli Enterprise
Norton AntiVirus Plus 5.0 Tivoli IT Director
Norton AntiVirus Plus 5.0.3 for Macintosh (this includes the Administrator tool)
Norton AntiVirus Plus 4.04 for Netware
Norton System Center 3.1

Upgrades/updates are included for one year.

The software suite is designed to protect desktop computers, laptops, network servers, Internet email gateways, and firewalls against all sources of potential virus threats.

At the desktop level, Norton AntiVirus Solution protects against potential virus corruptions from Internet downloads, floppy disks, email attachments, shared files, compressed files, CD-ROMs and networked hard disks. It operates at all times, as a background application, without slowing other applications.

At the server level, the software suite:

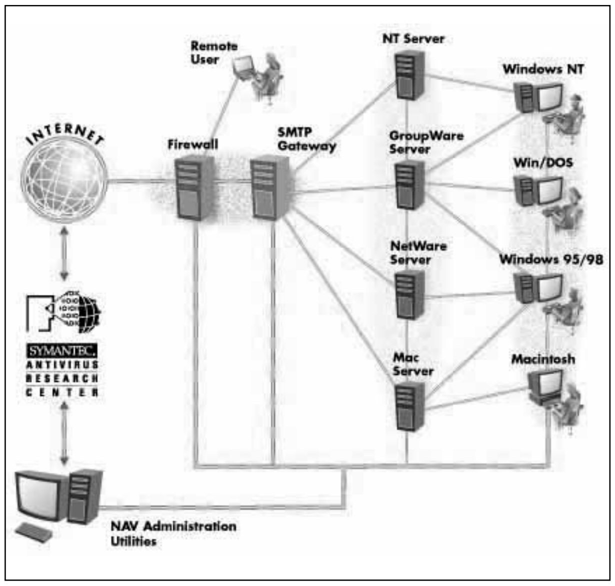
- Provides "real-time, scheduled and on-demand scanning to protect against virus transmissions within servers and workgroups running Novell NetWare, Windows NT Server, Microsoft Exchange and Lotus Notes."
- Affords the ability, through a centralized and flexible reporting system, to send alert messages to network administrators using a variety of alerting methods.
- Includes access to the Norton System Center (*http://www.symantec.com/sabu/nsc/index.html*), which allows network administrators to easily and automatically distribute, configure, monitor, update, and centrally manage Symantec software. It also makes it possible to quickly identify non-compliant machines and launch remote virus scans.

Norton AntiVirus Administrator for the Macintosh can be used to install, track, and update virus protection for all Macintoshes on a network.

CDs Available for Home Use

Norton AntiVirus CDs are available for home use by faculty and staff. They can be purchased at the UCD Bookstore Computer Shop. (We are negotiating an add-on agreement to include student use for Norton AntiVirus Desktop software.)

Each CD is priced at $3.50 (to cover CD duplication costs) and includes one license. Departments can also purchase these CDs, but system administrators should email the Site License Coordinator (*itslc@ucdavis.edu*) the number of computers on which they will install the software (if they haven't done so already).



The graphic above demonstrates how Norton's complete solution suite protects valuable data from unforgiving viruses.

Before You Install

We recommend you uninstall any other anti-virus

see License on page 7

Q. Is there a policy somewhere that gives the rules on linking to, and/or endorsing, a company on an official UCD Web site? What about from the other side: Is there a problem if a company uses the UCD logo and states that we endorse them? I thought I saw a draft of something awhile back addressing these and other Web-related issues.

— Asked recently on the Technology Support Program list

A. Timely question. The UC Davis World Wide Web Policy Committee is addressing these and other Web-related issues. The committee is composed of faculty, staff, and administration representatives with a shared interest in how the Web can be used effectively and responsibly in furthering UCD's mission of teaching, research, and public service.

Committee members have recently drafted a proposed UCD Policy and Procedures document on Web pages. The draft provides guidelines on the use of Internet resources for the conduct of university business and on Web page contents. Once approved, the policy will be posted on the Web at *http://mrak.ucdavis.edu/web-mans/ppm/welcome.htm* (look for Section 310-70). Directly relevant to the question at hand are the following excerpts from the draft policy:

Advertising: "Information on campus pages that suggests that the University endorses any commercial enterprise must be avoided. The use of commercial corporate identifying symbols or logos on campus pages may be appropriate only when the University has a contractual arrangement with the subject organization (1) for support of teaching, research, or public service activities or (2) for the delivery of services or products to UCD, when the use is beneficial to the delivery of said services or products. Web publishers may acknowledge donations or contributions by creating links to selected organizations/corporations that are contributors to UCD. Links to noncommercial sites, and public-service pages of commercial sites, are allowed. For relevant policies, see Section 270-25."

Use of University seals and logos: They are permitted on "official" UCD Web pages, (i.e., those maintained by the Public Communications Office), and on "unit" pages, (i.e., academic or administrative units). They are not permitted on pages owned by "affiliated organizations, individual faculty, students, or staff." The draft also refers readers to the existing policies on the use of the University name and seal (Section 310-65) and logo (UC Davis Publication Standards Guide).

One class of exceptions to the rule barring "affiliated" pages from using campus seals and logos: Registered student organizations, particularly sports-related groups like the Aggie Pack, will be allowed to use the new athletic logos and marks unveiled at the Aggie Auction on May 1.

Jan Conroy, manager, Editorial/Design, and Pat Kava, manager, Client Services, IT-Information Resources, contributed to this article.

License: *Software free fo charge*

continued from page 6

program(s) before you install Norton AntiVirus software. This will lower the possibilities of conflicts between the programs.

And the Good News Is. . .

The software is available to campus departments, staff, and faculty free of charge. For specific instructions on how to obtain the software, see the Site License Web page at *http://irlinux.ucdavis.edu/SLC/software/nortonav/nav.html*

Norton 2000 Corporate Edition

If you're like most people these days, you're trying to protect your laptops and desktop computers from Year 2000 problems. To help Year 2000 Coordinators address century-date issues — including data, applications, and BIOS vulnerabilities — the Division of Information Technology has recently purchased a set of Norton 2000 licenses.

Key Features

Norton 2000, available for Windows 95, 98 and NT, checks a computer's BIOS and applications for Y2K compliance problems. According to specifications provided by Symantec, Norton 2000:

- Identifies, prioritizes, and reports on two-digit date calculation anomalies in spreadsheet cells and formulas, database fields and forms, and text
- Scans all installed applications on a PC and audits them against a database of known Year 2000 problems
- Indicates where and how to obtain any known fixes or patches
- Tests the PC's BIOS and reports on its Year 2000 readiness
- Fixes the BIOS in many cases to bring it up to Year 2000 requirements.

Departmental Licenses

Five Norton 2000 licenses will be distributed at no charge to campus departments through their Year 2000 Coordinators. If a department requires more than the initial five free licenses, IT will coordinate an additional license purchase. However, there will be a charge of $12.99 for each license beyond the initial five, and we will need to purchase a minimum of 1,000 additional licenses. This information has been forwarded by email to campus Y2K Coordinators and Technology Support Coordinators (TSCs). Please contact your Y2K Coordinator or TSC if you have questions. You may also email the Site License Coordinator at *itslc@ucdavis.edu*.

Home Use

This agreement does not make provisions for home use. Faculty, staff and students can purchase Norton 2000 at the UCD Bookstore Computer Shop for $39.99.

For more information on Norton 2000, see *http://www.symantec.com/sabu/n2000/index.html*. For information on the Year 2000 Problem, see *http://y2k.ucdavis.edu*.

Are You a Wareforce Customer?

Wareforce has been the UC outside software reseller, distributing Microsoft, Lotus, Timbuktu, Apple, Filemaker Pro and Homepage products, for almost 3 years. Based on input from UC customers, the Office of the President has decided to conduct a search for a new outside reseller/distributor. Requests for Proposals have been sent to more than 15 distributors, including Wareforce, and we are waiting for the responses.

While changing to a new outside distributor may cause transition problems, these will be weighed against the problems many Wareforce customers have experienced. Some customers, for example, have reported receiving inaccurate information from Wareforce employees, sometimes taking weeks to get back to a caller. In addition, sketchy as well as lengthy, product delivery dates have been reported.

If you have an opinion or comment, either positive or negative, about Wareforce services, please email them to me at *itslc@ucddavis.edu*. Wareforce's Web site can be found at *http://www.wareforce.com/*.

Leigh Ann Giles is the Campus Site License Coordinator. She can be reached at itslc@ucdavis.edu.

Email: *Many complaints each month*

continued from page 2

tively for others).

3. Complain to the spammer's Internet Service Provider (ISP), but make sure you know how to read headers, so you're complaining to the right person.

- Open the message and expand the headers (see sidebar).
- Forward the message with full headers to *abuse@* or *postmaster@* followed by the ISP's domain.

4. Report it to *abuse@ucdavis.edu*.

- Open the message and expand the headers (see sidebar).
- Forward the message with full headers to *abuse@ucdavis.edu*.

To ensure that action is taken against the appropriate entity, the forwarded message must contain the full headers. Many of these complaints are investigated each month, so if you do not get a personal response immediately, please understand that it doesn't mean the complaint is being ignored.

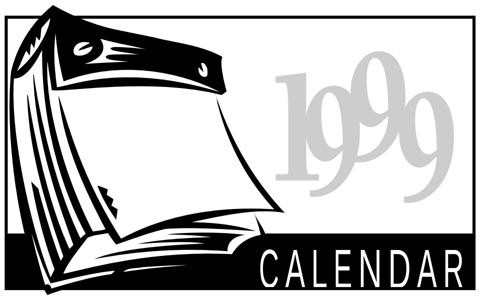
Ann Mansker is a member of the Incident Response and Reporting team. She is also assistant postmaster and an IT representative with the Technology Support Program (TSP).

Resources:

Coalition Against Unsolicited Commercial Email:
http://www.cauce.org

Expanding Headers

- In Eudora: Open the message and click on the "blah, blah, blah" icon in the bar directly above the text.
- In Pine: Open the message and press h (upper or lower case).
- In Outlook: Open the message, go to the View menu and select Message Header. Then click on the Options tab. The headers will appear on the options page. You'll need to cut and paste them into the body of your message before forwarding the whole assemblage.



http://it.ucdavis.edu/itcalendar/

May

4 ◆ Fundamentals of Excel: 8:30 a.m.-noon, TB 134.

5 ◆ Hot Topics in Computer Graphics/Animation/Video:Noon-1 p.m., Cabernet Room, Silo.

◆ Fundamentals of Windows 95: 1:30-5 p.m., TB 135.

6 ❑ Melvyl, Part 2: 10-10:50 a.m., 163 Shields Library.

10 ❑ Melvyl, Part 1: 2:10 - 3:00 p.m., 163 Shields Library.

12 ◆ Fundamentals of Access: 1:30-4:30 p.m., TB 135.

❑ Internet - Web Searching: 3:10 - 4 p.m., 163 Shields Library.

13 ❑ Melvyl, Part 1: 3:10 - 4 p.m., 163 Shields Library.

17 ◆ Designing an Access Database: 9:00 a.m.-4:00 p.m., TB 135.

18 ❑ Internet - Web Searching: 3:10 - 4 p.m., 163 Shields Library.

19 ◆ Fundamentals of Access: 1:30-4:30 p.m., TB 135.

20 ◆ Fundamentals of Netscape: 1:30-4:30 p.m., TB 134.

❑ Bibliographies for Research Papers: 3:10 - 4 p.m., 163 Shields Library.

24 ◆ Access Queries & SQL: 1:30-4:30 p.m., TB 135.

26 ◆ Fundamentals of Windows NT: 1:30-5 p.m., TB 135.

❑ Melvyl, Part 1: 11 - 11:50 a.m., 163 Shields Library.

27 Look Smart! Find jobs on the Web!: Internship and Career Center Workshop, 1-2 p.m., 27 Olson.

28 ❑ Bibliographies for Research Papers: 3:10 - 4 p.m., 163 Shields Library.

June

1 ◆ Fundamentals of Access: 1:30-4:30 p.m., TB 135.

Look Smart! Find jobs on the Web!: Internship and Career Center Workshop, 2-3 p.m., 27 Olson.

3 ◆ Web Publishing: Tables: 8:30-11:30 a.m., TB 134.

❑ Melvyl, Part 1: 3:10 - 4 p.m., 163 Shields Library.

Key to Classes & Seminars

❑ Library Instruction Programs: *LibraryClass@ucdavis.edu* or 752-4381.

◆ Staff Development & Professional Services (SD&PS): Enroll online at *http://sdps.ucdavis.edu*. Call 752-1766 for an application or catalog.

CUMREC '99

Conference Proposes to Look to 2000 and Beyond

The CUMREC (College and University Computer Users Association) annual conference is the longest running continuing conference devoted to promoting the understanding and use of information technology in higher education. This year's conference, scheduled May 9-12 in San Antonio, Texas, has a an impressive lineup of speakers, presenters, corporate participants, and social activities. Here's a sample of what you can expect.

Presentations

There are more than 55 presentations. Topics include:

- Building Information Out of Data
- Partnerships for Creating an Online Learning Environment
- Infrastructure for the Intranet
- Grading Programs for Instructors
- Functional Reengineering of a Purchasing Card System
- Collaboration Among Faculty, Students, Information Systems, and Administration
- Accessing Legacy Data for the Web Applications
- Privacy Policies: Who Needs Them?
- Facilitating Access to Management Information
- Developing and Implementing a Web-based Teaching and Learning Experience.

Featured Speakers

- Brian L. Hawkins, president of EDUCAUSE, will open the conference with future expectations for technology in higher education and CUMREC members' roles in that future.
- John E. Bucher, director of computing at Oberlin College, will explore the reasons behind rising customer expectations and how our technology staffs can work to shape these expectations in positive ways.
- Carl W. Jacobson, director of MIS at the University of Delaware, will focus on the issues of Web refreshment, institutional presentation, and the ways in which the Web changes how we do business and how our customers make decisions.
- Concluding the conference will be Baylor Professor Richard Couey with a lighthearted look at how to reduce stressin "today's high-tech society."

Online registration: *http://www.cumrec.com/cumrec99/*

MP3s: *Sentence can be stiff*

continued from page 3

"In general, computer misuse cases are referred to IT and SJA when system administrators notice interference with normal system operations," says Dudley, who is not allowed to discuss particular cases. "A lot of traffic through a Web site or an FTP site would be one cause.

"Most students know they are doing something they shouldn't," says Dudley, continuing. "They may not think it is a big deal, nor realize that there are consequences to violating campus policy concerning the use of university resources.

"Access to computing resources at UC Davis is a privilege. That privilege needs to be used responsibly or else one may lose it," he says. "(One) can also risk their future as a UC Davis student. Most ResNet misuse cases involve MP3 sites."

Anyone found guilty of willfully infringing a copyrighted work can be sentenced for up to five years imprisonment, fined up to $250,000, or both.

"I ended up getting probation, deferred suspension, no ResNet connection for one year, and 15 hours of community service," says Bradley. "I did have the option of rejecting that contract but then I would have a formal hearing and there was no way of knowing what would happen there; I may have ended up with more severe punishments."

Resources:

UC Davis Computer Acceptable Use Policy: http:*//www.ucdavis.edu/html*

Recording Industry Association of America: *http://www.riaa.com/*

One legal MP3 site: *http://www.mp3.com/*

IT Quick Tip on MP3s: *http://it.ucdavis.edu/pubs/quicktips/*

Myths: *Fewer sales result*

continued from page 3

right owner to decide how their music will be heard, distributed, and promoted. Furthermore, approximately 15 percent of record sales support new and emerging artists who are being recorded. Fewer sales mean less money for new music. To an emerging artist, every sale counts.

I'll never get caught anyway; nobody ever does.

FALSE. The RIAA is continually combing all facets of the Internet, looking for Web and FTP sites that distribute MP3s.

Provided by and used with permission of the Recording Industry Association of America. Excerpted from a Quick Tip available at http://it.ucdavis.edu/pubs/quicktips/.

IT TIMES

The IT Times is published by the Division of Information Technology, University of California, Davis, to inform the campus community and others of information technology services, facilities, and activities at UC Davis. It is distributed free of charge to members of the user community and to other universities. Use of trade or corporation names in this publication does not constitute endorsement by the University of California, Davis. IT Times articles may be reprinted as long as the source is accurately quoted and credited.

Editor: Babette Schmitt (530) 752-5965
Senior Writer: Matt Peters
Webmaster / Desktop Publisher: Richard Darsie
Designer: Marianne Post
Digital Imaging: Gabriel Unda

Email: *itpubs@ucdavis.edu* Web: *http://it.ucdavis.edu/it.times/*

Information Technology UCDavis