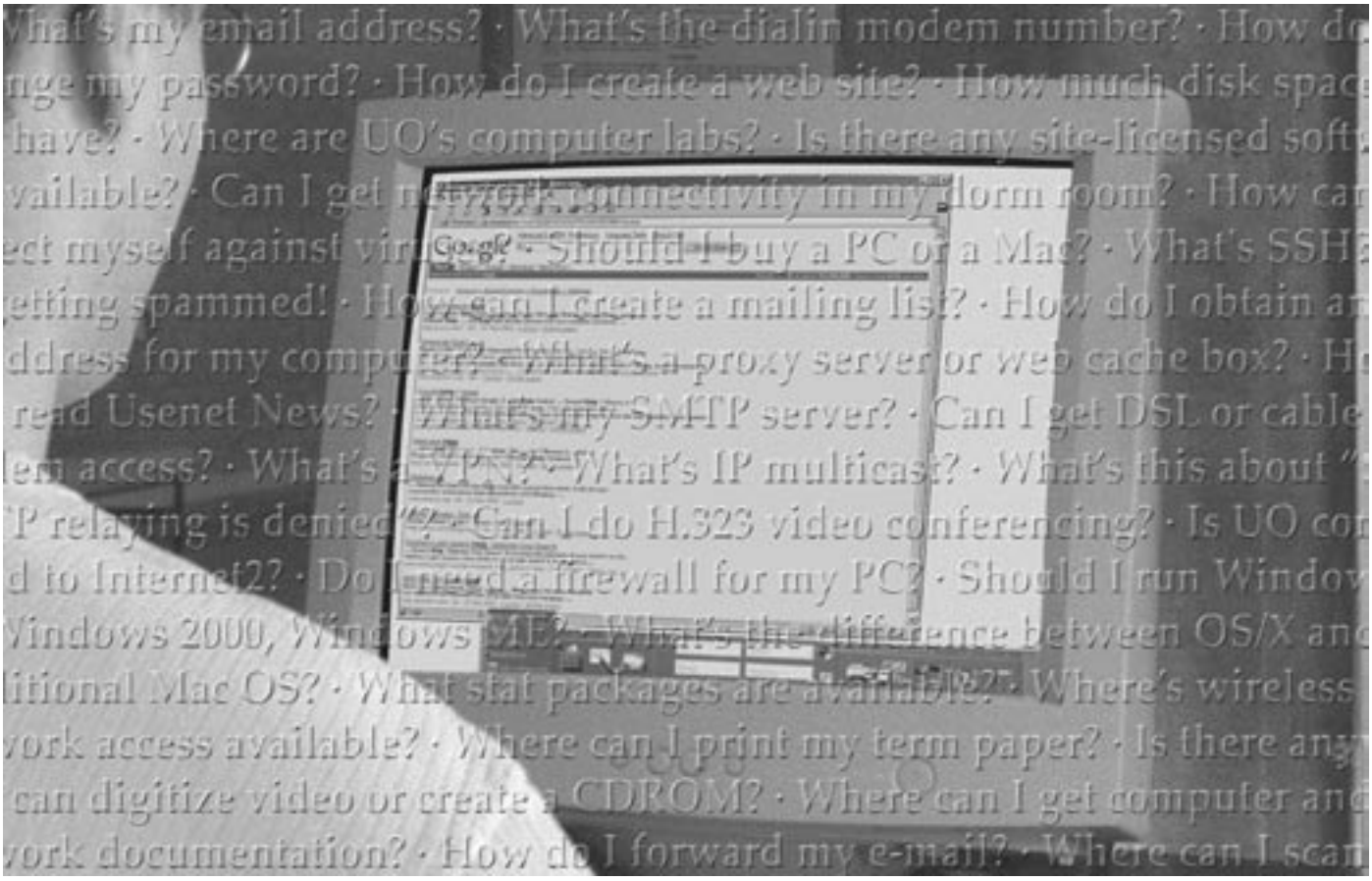
University of Oregon

COMPUTING NEWS

Fall 2002



New to campus? Find out about campus computing resources in the "New User Section," pages 2-10.

IN THIS ISSUE...

Welcome to Campus!

How to Get Started Using Your UO Computing Account

When you register for classes, we automatically generate a computing account for you that consists of a username and password. Your computing account provides both email and dialin access.

(If for some reason you don't have a UO computing account, pick up a copy of "How to Get a Computing Account." This handout is available in the Documents Room Library (175 McKenzie Hall), and online at **http://cc.uoregon.edu/policy/get_account.html**)

UNIVERSITY OF OREGON

COMPUTING CENTER

COMPUTING NEWS

VOL. 17 #4

Computing News is published quarterly by the User Services and Network Applications staff of the Computing Center, 1212 University of Oregon, Eugene, OR 97403.

Contact:
Joyce Winslow
jwins@oregon.uoregon.edu
Joe St Sauver, Ph.D.
Director, User Services
and Network Applications
joe@oregon.uoregon.edu

Website:
http://cc.uoregon.edu/cnews/

Telephone: (541) 346-1724

Photography: Dave Ragsdale

If you're wondering how to get started using your email account, read on.

There are three ways to get your email information:

- via DuckWeb (**http://duckweb.uoregon.edu/**)
- in person, by going to the Microcomputer Support Center (151 McKenzie Hall) and presenting your photo I.D.
- by accessing the AUTHORIZE program, either from your web browser (**https://password.uoregon.edu/authorize/**), or by logging into the campus network via SSH Secure Shell (see **http://micro.uoregon.edu/security/ssh/shell.html** for instructions).

What About Passwords?

We recommend you select your own password instead of using the one that's generated for you when you register for classes. Here's how:

1. Open your network browser (e.g., Netscape, Internet Explorer) and go to **https://password.uoregon.edu/**

2. If you remember your old password, enter your username and old password in the spaces provided. Type in your new password and enter it again for verification.

3. If you don't know your old password, you'll need to know your student ID number and PAC code. Go to **https://password.uoregon.edu/authorize/** Enter your student ID and PAC code in the spaces provided, and follow the instructions for creating a new password.

Password security: Passwords should be 6 to 14 characters long and must be very secure. We recommend choosing a password that includes a mixture of letters, numbers, and mixed case. Dictionary words and any part of your name are not allowed. For more detailed information on password policy, see **http://cc.uoregon.edu/policy/passwd_policy.html**

What About Dialing In From Off-Campus?

Your computing account username and password are the same ones you'll use for dialing in via modem. The only difference you'll notice is that you must type in your full username address to dial in, including your account's hostname (e.g., **jersmith@gladstone.uoregon.edu** or **jersmith@darkwing.uoregon.edu**)

The modem number for accessing UOnet, the campus network, is **225-2200**.

Note: Your modem access is for casual use—no more than a few hours a day on average. If you need dedicated or near-dedicated network access, you'll want to contact a commercial Internet Service Provider.

What About Wireless ?

You can also access UOnet throughout several public areas on campus by inserting any 802.11b card in your laptop computer. For more information on campus wireless and current areas of coverage, see

http://micro.uoregon.edu/wireless/

Got Extras?

If your campus department receives surplus copies of *Computing News*, you may return them to the UO Computing Center for redistribution.

Connecting to UOnet from Campus Housing

Every room in every UO residence hall has an ethernet connection (ResNet). You don't need a modem to use it, but you will need an ethernet card. If you are a UO student living in the Residence Halls, University Housing can not only sell you an ethernet card for your computer, but install it and set it up free of charge. For more information about ResNet and details about purchasing an ethernet card, see **http://www.housing.uoregon.edu/resnet/**

Get Your Copy of Duckware 2002

As always, this year's Duckware CD is packed with the latest software and documentation to help you with computing at the UO

It's fall, and time for a new edition of Duckware!

With the aid of a generous grant from Sony Disc Manufacturing, the Computing Center's Microcomputer Services group has created the Duckware 2002 CD, which is packed with the latest software and documentation to help you with computing at the UO.

Duckware 2002 is available for both Windows and Mac OS and is free to current UO students, faculty and staff. Among other useful items, this year's Duckware CD includes

- Norton AntiVirus 2002 to ward off computer viruses
- step-by-step instructions for using the UO's modem pool, wireless network, and VPN connections
- SSH secure shell for encrypted network connections
- IP/TV for viewing such multicast broadcasts as live news, computer conferences and conventions, prerecorded NASA flights, and Internet Radio
- Internet Explorer 6 and Mozilla web browsers (among others)
- a newsgroup client (Free Agent for Windows, YA-NewsWatcher for Mac OS 8 and above, and MT-NewsWatcher for Mac OS X)

New this year: The Macintosh version of Duckware 2002 includes a freeware secure FTP client, Fugu, which had not been previously available for Mac OS X.

System Requirements

PC users: To use Duckware 2002 for Windows, you'll need Windows 98, ME, 2000, or XP.

Mac users: The Macintosh version of Duckware is compatible with Mac OS 8.6, 9, and OS X.

Where to Get Duckware

Students, faculty and staff may pick up a copy of the Duckware 2002 CD at one of the following campus locations:

- Microcomputer Support Center (151 McKenzie Hall)
- Documents Room Library (175 McKenzie Hall)
- CC-McKenzie Lab (101 McKenzie Hall)
- CC-EMU Lab (22 EMU)
- CC-Klamath Lab (B13 Klamath Hall)
- CC-Millrace Lab (113 Millrace I)
- Knight Library Information Technology Center (ITC)
- Science Library Information Technology Center (ITC)

Campus Housing Distribution. Students living in campus housing can get Duckware at Residence Hall and Family Housing area desks in the University Inn, Carson, Spencer View and Westmoreland.

Reuse and Recycling

If you decide you no longer want your copy of Duckware 2002, please don't throw it away! We'll gladly take it back and give it to someone else. Just drop it off at the Microcomputer Support Center, or mail it via campus mail to Microcomputer Services, 151 McKenzie Hall.

Questions?

For more Duckware help or information, call the Microcomputer Support Center at **346-4412** or email *microhelp@lists.uoregon.edu*

You can also visit the Support Center in 151 McKenzie Hall on weekdays from 9 A.M. to 5 P.M., or check out their website at **http://micro.uoregon.edu/**

A Special Thank-You to Sony

Spencer Smith
Microcomputer Support Specialist
spencera@oregon.uoregon.edu

For the third consecutive year, Sony Disk Manufacturing has very graciously donated CD duplication services for our annual Duckware CD-ROM.

Sony's duplication of 15,000 Duckware CDs represents a contribution of nearly $10,000 to the UO campus community, and is of crucial importance to the university's ongoing computing and networking support efforts.

We very much appreciate Sony's donation of these services, and as always, it was a pleasure to work with Sony's extremely competent, professional, and talented staff.

Thank you, Sony!

New to Campus? Get Acquainted with

Help Desk consultants in 151 McKenzie are on hand to assist you with a wide range of computing questions and problems.

Consulting Help for Your PC or Mac, and More…

If you have Windows or Macintosh problems of almost any description, Microcomputer Services can help. Located on the ground floor of McKenzie Hall in Room 151, this facility is staffed with consultants who can answer questions about a variety of hardware and software conundrums, including

- how to connect to the Internet from home or on campus
- new student computing accounts information
- password problems
- how to transfer files
- virus problems and protection
- system software configuration, troubleshooting, and installation
- damaged files and disks
- public domain software distribution

Student Accounts. Microcomputer Services staff can help with student accounts and password changes. New students can also obtain their account information via DuckWeb (**http://duckweb.uoregon.edu/**) using their student ID number and PAC code.

For complete information about student accounts, see **http://micro.uoregon.edu/getconnected/** or pick up a copy of the handout "New Students: Get Online!" in 175 McKenzie (the Computing Center's Documents Room Library).

Machine Check-In. For customers who encounter particularly complex or hard-to-diagnose problems, Microcomputer Services offers a machine check-in service that costs $60.00/hour, with a minimum charge of $30.00. Typical problems include those that require reinstallation of operating system software, diagnosis of corrupt data, virus removal, and resolution of particularly difficult hardware conflicts that manifest themselves in software.

Multimedia Facilities

Microcomputer Services also has public stations in 151 McKenzie for scanning, CD copying and burning, and digital video acquisitions. (As in all electronic copying activities, copyright restrictions must be observed.) These services are available to UO students, faculty, and staff. Current services include:

PC Station (Windows XP, 45GB disk, 256MB RAM, Firewire support, Plextor 8x20 SCSI CD-R, Viewsonic G790 19" monitor):

- scanning: OCR (Optical Character Recognition), regular, and slide
- CD-ROM creation and duplication
- video in and out
- direct VHS/S-VHS into MPEG-1 in real time
- direct VHS/S-VHS into MPEG-2 in real time
- Some editing features using Adobe Premiere and Photoshop
- ZIP (100MB) and JAZ (2GB) drives

Some UO Computing Resources

Mac Station (Mac OS X 10.2, dual 1 GHz processor, 512MB RAM, 75GB hard drive, CD-RW, DVD-R, Firewire support):

- scanning
- video in and out
- video editing with iMovie and Adobe Premiere
- CD-ROM creation and duplication
- DVD creation using iDVD
- some editing features using Adobe Photoshop
- ZIP (100MB) and JAZ (2GB) drives

The PC is outfitted with two 18.1 GB, high-speed SCSI hard drives to facilitate the capture of large video files. To speed the transfer of data over UOnet, both the PC and Mac machines have 100Mb/sec Ethernet connections. Each station has a two-hour time limit and is available on a first come, first served basis.

Storage media. You may purchase up to 5 CD-R disks at $2 each in 151 McKenzie Hall if you wish. If you need more, you'll want to purchase them before coming in. ZIP or JAZ cartridges are not available.

Help. Microcomputer Services staff is available to assist you with basic use and start-up questions. If you need in-depth training on such skills as how to create CD-ROMs, capture video, or edit images, you will probably want to take some classes first.

For more in formation, contact Microcomputer Services at **(541) 346-4412** Monday through Friday, 9 A.M. to 5 P.M.

Instructional and Drop-in Computing Labs on Campus

Instructional labs. The Computing Center has four computing labs available for use by instructors. Windows labs are located in B26 Klamath and 101A McKenzie, and Macintosh labs in B13 Klamath and 113 Millrace. Each lab is equipped with 20 to 24 computers and a variety of software. We recently installed the Macromedia Studio MX software, including Flash and Dreamweaver, and are also installing PhotoShop 7, Illustrator 10, Premiere 6, GoLive 6, and the latest MS Office software.

Reserving a lab for instructional use. Instructional labs are generally reserved for classes and lab sessions several terms prior to the term needed; however, there are a few times that are still available for instructional use. If you are interested in reserving a lab, please contact Mary Bradley (*mbradley@oregon.uoregon.edu*, **346-1737**).

Drop-in labs. Besides instructional space, the Computing Center also maintains drop-in labs. There are drop-in lab facilities at each of the instructional sites, plus a large drop-in lab located in the basement of the EMU:

CC-EMU Lab. 22 EMU (in the basement near the Recreation Center and Arcade). **346-1769**.

Millrace I Lab.113 Millrace I. **346-0316**

CC-Klamath Lab. Located in Klamath B13 and B26. **346-4781**

CC-McKenzie Lab. 101 McKenzie Hall (ground floor). **346-0787**

Other Campus Computing Labs:

Knight Library ITC - **346-1935**
Science Library ITC - **346-1331**
Social Science Instructional Lab - **346-2547**

For complete details about the software and services in all of these labs, as well as other computing labs on campus, see **http://cc.uoregon.edu/campuslabs.html**

The CC-McKenzie drop-in lab in 101 McKenzie Hall is open Monday through Thursday from 8 A.M. to 11:30 P.M., and from 8 A.M. to 6 P.M. on Friday and 1 P.M. to 9 P.M. on Sunday during the term.

Electronics Shop Provides Extensive Computer Repair, Upgrade Services

E-Shop technicians at work: Robert Bennett restores a laptop while Rob Jaques assists a caller.

Conveniently located on campus in 151 McKenzie Hall, the "E-Shop" offers extensive personal computer hardware support and repair services to UO students, faculty, and staff. Its technicians are experienced with many brands of microcomputers, laptops, and peripherals, including Apple and Windows/Intel machines, and can also offer advice regarding upgrades.

E-Shop Services include:

Apple Repair. The shop is a Level 1 Apple-authorized service center and can perform warranty, AppleCare, and out-of-warranty repairs on nearly all Mac models and peripherals.

Windows/Intel Repair. A Dell certified Tier 1 Service Provider, the shop can perform non-warranty repairs on all desktop and laptop models. On-campus warranty and out-of-warranty service is also provided on all Tangent computers, and non-warranty repairs are offered for most Windows/Intel machines.

Upgrades. E-Shop technicians can help you determine the best and most cost-effective way to upgrade your machine. The shop keeps memory in stock for virtually all Mac and Windows/Intel-based desktop computers, and other items can be ordered upon request.

Custom Systems (including backup solutions such as Firewire/USB and Zip or CD-RW drives). If you need a backup solution or a custom system configuration, like a server with multiple SCSI controllers and mirrored disk drives, talk to the technicians. The shop may be able to build you a machine at considerable savings.

Upgrades and out-of-warranty repairs are charged on a time-and-materials basis. The current labor rate is $60/hour, with a half-hour minimum.

Parts. If you need more cables, computer batteries, power strips, ethernet cards, or extension cords, you'll find a wide selection at the shop. The shop stocks ethernet cables as well as cables for printers and monitors, so you won't have to wait or travel far to get what you need.

Hours and Policies. The shop is open from 8 A.M. to 5 P.M. Monday through Friday, except holidays. Parking is available in the McKenzie parking lot on the west side of the building.

All shop services are available on a first-come, first-served, carry-in basis. On weekdays, bring your computer equipment to 151 McKenzie Hall and check it in with the receptionist. UO Bookstore customers can also drop off equipment from 10 A.M. to 6 P.M. Saturday and from noon to 6 P.M. Sunday at the Bookstore's "Digital Duck" department. The E-Shop will call you when the work has been completed, and you may pick up your machine at the McKenzie Hall reception desk.

Who to Contact. If you have any questions concerning repairs or upgrades, send an email message to *hardwarehelp@oregon.uoregon.edu*, or call Rob Jaques or Robert Bennett at **346-3548**.

Technical Information and Training Resources: the Computing Center Documents Room

Looking for a book on Java, a copy of Linux, or a video on Photoshop? The Computing Center's Documents Room Library (175 McKenzie) offers a collection of books, magazines, CDs, and instructional videos on a wide range of popular computing subjects. You can search its catalog 24 hours a day at **http://docsrm.uoregon.edu/**

You can borrow books for two weeks, videos for one week, and magazines for two days.

Workshops-to-Go. If you're feeling the need to update your computer skills but are having trouble fitting a workshop or class into your busy schedule, consider taking a video workshop on VHS tape or CD-ROM.

The Documents Room has recently added a complete set of video workshops on Microsoft Office XP. You'll find beginning, intermediate, and advanced tapes on Word, Access, Excel, PowerPoint, and Outlook. Each tape includes about two hours of instruction by experts skilled in software training.

Other recent acquisitions include two tapes on Photoshop 7 ("Adobe Photoshop for Beginners" and "Photoshop 7.0 Power Session," both featuring Scott Kelby, the editor of *Photoshop User Magazine*), and the tape "Illustrator 10 from the Ground Up" by Felix Nelson, creative director of *Photoshop User*.

Mac users looking for instruction on Mac OS X will find a four-disk set of workshops on CD-ROMs that they can play on their own computers using QuickTime. These CDs feature high-quality visuals, especially noticeable in the shots of computer screens.

Many other instructional videos are also available in the Documents Room. To see a complete list, go to **http://docsrm.uoregon.edu/**, move the drop-down menu from "All Words" to "Medium" and type in "Video." Then hit "search."

The videos and CD-ROMs circulate for one week and are renewable if no other user has requested the title.

Hours are 9:30 A.M. to 5 P.M. Monday through Friday. Call **346-4406** for more information or visit the Documents Room website at **http://darkwing.uoregon.edu/~docsrm/**

The Computing Center Documents Room (175 McKenzie) provides a comfortable setting for study and catching up on the latest technological developments.

Large Timesharing Systems at the UO

Your UO computing account gives you access to one or more large timesharing systems. To help you choose the system that best suits your needs, we've described them in some detail below

Faculty/Staff

Faculty and staff will normally use Darkwing, a large shared Sun Enterprise 5500 system targeted for compute-intensive academic applications.

If you have accounts on additional machines, please be sure to routinely check your email on all systems, or forward your email from your less preferred account to your favorite account.

Undergraduate Students

Undergraduate student accounts are automatically created on Gladstone, a large Sun Enterprise 5500 Unix system.

Gladstone accounts can be used for electronic mail and serving personal web pages. We also offer an expanded range of academic software on Gladstone, such as SAS and Mathematica (see software chart on page 9).

Graduate Students

Graduate students automatically have accounts created for them on Darkwing; however, if they wish, they can also authorize themselves for an account on Gladstone.

Administrative Systems

Daisy. Daisy is a large Alpha administrative system running OpenVMS/AXP. The primary application running on Daisy is BANNER, an administrative application environment based on Oracle, a popular large system database. Access to Daisy is restricted to staff members who are performing administrative tasks like grade processing and payroll.

Dialin Access?

Your account on Darkwing or Gladstone enables you to dial in from off campus to the university's modem pool (see "What About Dialing In From Off-Campus?" on page 2.) The modem number for accessing UOnet, the campus network, is **225-2200.**

Your modem access is for casual use—no more than a few hours a day on average. If you need dedicated or near-dedicated network access, you will want to contact a commercial Internet Service Provider. One list of ISPs is available at **http://www.thelist.com/**

Special Accounts for Classes and Departments

If you're teaching an undergraduate class and your students need to access software available only on Darkwing, temporary accounts can be created for their use. For more information, contact Connie French at **346-1738**.

Departments or university-recognized institutes, labs, or organizations can arrange for a departmental account. Such accounts are offered solely to provide an authoritative and unchanging home for departmental web pages and official departmental email, and must be officially requested by the department head or institute administrator.

Acceptable Use. Finally, please note that all use of university computing resources is subject to the university's Acceptable Use Policy, which is available in printed format from the Computing Center Documents Room (175 McKenzie Hall), or online at **http://cc.uoregon.edu/policy/**

Large Systems Consulting Help

If you have any questions about using the UO's large timesharing computers, contact the large systems consulting group in Rooms 225-239 Computing Center (**346-1758**). They can help with questions about email, multimedia delivery, scientific and CGI programming, and web page development. For more information about these services, see **http://cc.uoregon.edu/unixvmsconsulting.html**

Site-Licensed Software

The UO has site licenses for a number of software packages you can use on your campus workstation, including:

- **Norton Antivirus.** Available on the Duckware 2002 CD (see article on page 3). See also **http://www.symantec.com/avcenter/**
- **SAS.** SAS users are allowed to install SAS on their PCs both at work and at home. Go to **http://sas.uoregon.edu/**
- **Mathematica.** See **http://darkwing.uoregon.edu/~hak/mathematica/**
- **ESRI** (GIS and mapping software such as ArcInfo, ArcView) See **http://www.esri.com/**
- I**MSL numerical libraries.** Contact Hans Kuhn at *hak@oregon.uoregon.edu*

Administrative Computing

The Administrative Services IT staff supports applications that are used by practically every department on campus, as well as some areas of the Oregon University System. They are specifically responsible for the SCT Banner applications such as A/R, Finance, Payroll, Student, Financial Aid, DuckWeb, DuckCall, and the data warehouses. In addition, they support many auxiliary administrative applications including the UO online directory, and systems in Housing, Student Health Center, Printing Services, and Facilities Services.

If you have any questions about Administrative Services, contact Susan Hilton (*hilton@oregon.uoregon.edu,* **346-1725**) or Jim Bohle (**346-1706**, *jbohle@oregon.uoregon.edu*).

Software on Darkwing and Gladstone		
Type of Software	**Darkwing**	**Gladstone**
Statistics Packages	sas, eqs, lindo, bmdp, spss, rats/estima, Splus, minitab	sas, eqs, spss, bmdp, Splus, rats/estima, minitab
Text Editors	pico vi emacs and xemacs TeX and LATex eve	pico vi emacs and xemacs TeX and LATex eve
Network Software	ftp (remote file transfer) lynx (web browser) pine (email) trn, tin, nn (USENET News) ssh (secure login) pgp (encryption)	ftp (remote file transfer) lynx (web browser) pine (email) trn, tin, nn (USENET News) ssh (secure login) pgp (encryption)
X Window Only	netscape (web browser) xv (image manipulation) staroffice (Office Suite) acroread (Acrobat Reader)	netscape (web browser) xv (image manipulation) staroffice (Office Suite) acroread (Acrobat Reader)
Programming	cc and gcc c+ and g++ f77 (FORTRAN) pc (Pascal) IMSL Math/Stat Libraries NCAR fortran graphic libs Java developer's kit tcl/tk	cc and gcc c+ and g++ f77 (FORTRAN) pc (Pascal) IMSL Math/Stat Libraries NCAR fortran graphic libs Java developer's kit tcl/tk
Mathematics	mathematica, magma, matlab, maple	mathematica matlab
Miscellaneous	RealAudio server Adobe Acrobat distiller	RealAudio server Adobe Acrobat distiller

On the Road? Access Your UO Email via Secure UO Web Email at http://email.uoregon.edu/

Your UO computing account gives you access to secure, SSl-encrypted webmail at **http://email.uoregon.edu/**

UO web email is a good choice for new students and others who access their email from multiple locations. To use it, just open your web browser to **http://email.uoregon.edu/** and choose Gladstone or Darkwing as your email server. Enter your UO computing account username and password in the dialog box that opens, and you're on your way!

Another benefit of UO webmail is that you can use it in addition to your other favorite email clients like Eudora and Outlook without worrying about messages being moved around as they're read. For example, if you read and save Monday's mail with UO webmail, you'll be able to find all the messages you saved if you decide to open your mail with Eudora on Tuesday.

For step-by-step instructions on using UO web email, see the handout "Using Web-based Email on Gladstone and Darkwing," available online at **http://cc.uoregon.edu/glwebmail.html** and in the Computing Center Documents Room (175 McKenzie).

FAQs about Using Campus Cash for Printing in Computing Labs

Mary Bradley
Microcomputer Lab Coordinator
mbradley@oregon.uoregon.edu

This fall, you'll need to use your Campus Cash debit account to pay for printing in the Computing Center's public-access computing labs (CC-Millrace, CC-McKenzie, CC-EMU, and CC-Klamath). If you're unfamiliar with Campus Cash, see the "About Campus Cash" section at the bottom of the page.

The current fee for black and white laser printing is $.05 per page.

Below are answers to some frequently asked questions about the new laser printing policies:

- What was wrong with the old XCP copy card system?

First, the XCP system was used only for Library copying and printing. It required the UO Card Office to order an extra magnetic stripe on all ID cards, and payment could be made only in a few Library locations. Second, the card readers were old, trouble-prone, and due for replacement. Furthermore, the design of the card readers made it easy for patrons to forget their cards. The timing was right to move to a more reliable campuswide system.

- How do I use up the balance remaining on my old XCP copy card or UO I.D.?

Through fall term 2002, we are keeping a few XCP card readers available on copiers (not on laser printers). You may also stop by the Library Copy Service, 117 Knight Library, and transfer the balance to an established Campus Cash account.

- If the copiers or printers don't work and eat my money, how do I get a refund?

Contact the nearest service desk for a refund slip. If you have trouble with laser printing, in many cases staff can retrieve the job from the print queue and re-send it.

- Why do you charge students for printing anyway? Doesn't the Ed Tech Fee support free printing?

The UO Libraries have charged for printing since 1997 and the Computing Center labs are instituting charges for the first time this fall. Library printing outside of the ITCs was never supported by student fees.

Before charging mechanisms were put in place, heavy use of this "free" service resulted in significant cost overruns each year, with a high level of waste—50% of the paper used in labs was not claimed by users and had to be recycled. The increasing level of printing activity in labs and from public workstations could not be sustained without compromising other critical educational technology and information service programs.

All users are encouraged to learn about alternatives to printing (downloading, emailing search results to your Gladstone or Darkwing account, etc.**).** Staff at the public labs, ITCs, and library reference desks can help, and can refer you to appropriate workshops and other training resources.

About Campus Cash…

All UO students, faculty, and staff have a pre-established Campus Cash account. To activate your account online, go to **https://millrace.uoregon.edu/ccash/about_activate.html** Or, go in person to the UO Card Office on the ground floor of the EMU, or call (**541) 346-3113** (toll-free at **1-877-877-4635**).

You can add funds to your Campus Cash account at several locations and in a variety of ways (described online at **https://millrace.uoregon.edu/ccash/about_deposits.html**)

Here's a brief synopsis of your options:

1. Cash Registers:
Library Copy Service, 117 Knight Library
Daily Grind: ground floor Knight Library

2. Online, via the secure e-commerce server at
https://millrace.uoregon.edu/ccash/online.html

3. Credit or debit bank card: Instant deposit with approved credit limit or debit account balance

4. Charge to student account (UO students only): Requires 24 hours to validate account in good standing.

5. Departmental Cards: UO departments may purchase generic cards and establish Campus Cash accounts by Journal Voucher. Contact the UO Card Office at **346-3113** (**http://uocard.uoregon.edu/**)

Report lost or stolen cards:
https://millrace.uoregon.edu/ccash/about_lost.html

Secure Hotmail Alternative:

If your friends and family need a free email account, they might want to know about *MyRealBox*. This free email site offers SSL security, no ads and little or no spam, and 10 MB of storage (five times the amount provided by Hotmail). Another useful feature of *MyRealBox* is that you can access it via IMAP or POP.

To find out more about *MyRealBox* or to sign up for service, go to

https://www.myrealbox.com

A Note on NAV: Don't Panic if You Get a 'Subscription Expired' Message

Dan Albrich
Microcomputer Network Specialist
dalbrich@oregon.uoregon.edu

This year, an increasing number of UO users will see a message from Norton indicating that their virus definition subscription has expired.

If you're among them, don't worry, our site license is still intact. We have the LiveUpdate subscription code you need, along with steps and pictures describing how to install it, on our main antivirus web page at **http://micro.uoregon.edu/av/** (note that you must be connected to the UO network to access this resource).

Why the expiration notice? In previous years, Symantec's Norton AntiVirus (NAV) allowed you to install a new version on top of the old, automatically updating the subscription information for another year. Unfortunately, the newer versions of NAV no longer permit this type of installation. Users are now required to uninstall any prior version of the product—often a rather complex operation—before they can upgrade.

The new version for this year, Norton AntiVirus 2003, was not available at press time, and did not make it onto Duckware 2002.* NAV 2003 is very similar to last year's offering, with the exception of its ability to scan files transferred by instant messaging programs, which we don't recommend using anyway (see the Spring 2000 Computing News article "Be Aware of Security Issues with ICQ Instant Messaging" at **http://cc.uoregon.edu/cnews/spring2000/icq.html**).

***Note:** Symantec released NAV 2003 on September 4. Our initial testing indicates that it's easy to install on top of earlier versions, and it comes with another year of LiveUpdate. To install (UO restricted), go to* **ftp://public.uoregon.edu/software/AntiVirus/NAV2003.EXE** or check out a CD-ROM from the Documents Room.

Corporate edition update (NAV CE 8.0): Departments using the corporate edition of NAV will find the update in the AntiVirus/Corporate Edition folders on the "Software" volume of the Public server (**http://micro.uoregon.edu/pd/**)

What Should You Do if You Get an Expiration Notice?

If you get an expiration notice, you can either enter the new LiveUpdate code, or upgrade to the latest version of NAV.

Given the lack of a compelling reason to upgrade and the potential difficulty of the process, Microcomputer Services staff recommends that you simply enter the new LiveUpdate code when prompted to do so. See **http://micro.uoregon.edu/av/** for information about how to apply the subscription code.

Installing NAV 2003 (Windows only): As mentioned earlier, NAV 2003 was not available when we created this year's Duckware CD. If you prefer to install this updated version of NAV for Windows, you can get it from our public domain server (**http://micro.uoregon.edu/pd/**) or from the Documents Room in 175 McKenzie Hall.

Mac users: The NAV versions included on Duckware 2002 (NAV 7.2 for Mac OS 8 - 9.x and NAV 8.0 for Mac OS X) are still the most current Macintosh releases, so after you install the version that's appropriate for your needs, you won't need to update further.

The Future of Our Site License

We are currently in the final year of our three-year site license agreement with Symantec. The current license runs through July 2003, and Microcomputer Services will be investigating antivirus products this winter and spring. We anticipate entering into a new agreement for subsequent years, either a renewal of the Symantec Norton AntiVirus product or a new alternative product, depending on what sort of agreement can be reached.

Remember: KaZaA/Morpheus, Gnutella Rate Limited

Because popular peer-to-peer filesharing programs such as KaZaA/Morpheus and Gnutella slow network performance for everyone, the university has restricted the bandwidth available for their use. This limitation (equivalent to a T1 line) applies to both inbound and outbound traffic.

UO student, faculty, and staff also need to remember that all copyright provisions apply to audio or visual files exchanged over the Internet. Trafficking in copyrighted material without express permission from the copyright holder is a violation of the UO's Acceptable Use of Computing Resources and federal law, and may result in civil or criminal action or university sanctions.

For more information on the UO's acceptable use policy, see **http://cc.uoregon.edu/docs/acceptable_use.html** If you have questions concerning acceptable use, please contact Jon Miyake. (*miyake@darkwing.uoregon.edu*, **346-1635**).

Expand Your Options with Right-Clicking

Spend a few minutes exploring contextual menus

Patrick Chinn
Distributed Network Computing Consultant
pchinn@oregon.uoregon.edu

Take a look at your mouse. If you are using a computer running Windows, your mouse will have at least two buttons. It may even have a scroll wheel as well. You undoubtedly use the left mouse button with great frequency, but what about the right button?

Windows. In Windows, the right mouse button is the secret portal to new features. We all know that if you click twice with the left mouse button (also known as a double-click), it will open whatever you click on. Click once with the right button, however, and you get a menu.

This menu is called a contextual menu because the items in that menu will be different depending on the particular item you click (the context of the click). Right-clicking on a program produces different results than if you right-click on My Computer. (Take a couple of minutes to try it. What menu items show up consistently? What items change from object to object?)

Right-clicking in Windows will offer you a menu of choices that include Open, Create Shortcut, Delete, Rename and Properties. Most of these options are self-explanatory. Properties, however, unlock a host of configuration options.

As an example, right click on the Recycle Bin (in Windows) and select Properties from the contextual menu. In the window that appears you can (in Windows 98) perform the following actions:

- turn off the "Are you sure you want to delete this file?" warning message
- set Windows to delete files immediately
- set the amount of disk space Windows will set aside to store files in the recycle bin

Using the Properties option with files and folders will give you information like file size and creation date. You can even hide the file or folder by checking the "Hidden" option. (Note, however, that once you hide an item it is difficult to find it again to make it visible.)

Right-clicking also comes in handy when moving or copying items. If you right-click and drag a file, for instance, Windows will give you three options when you release the mouse button: Move Here, Copy Here and Create Shortcuts Here.

Mac OS. Mac OS users have a similar feature. With Apple's standard one button mouse, hold the Control key and click on an object to reveal a contextual menu. Some versions of Mac OS add a small menu icon to the pointer, providing immediate feedback when you press the Control key.

Apple's version of Properties is called "Get Info." This shows creation and modification dates and times, file size and comments. You can also lock a file to prevent it from being overwritten.

Mac OS X supports two-button mice right out of the box, so if you find yourself Control-clicking with frequency, buy yourself an inexpensive two-button USB mouse and enjoy.

Microsoft and Apple have continued to refine the function of contextual menus in their operating systems. Contextual menus in Mac OS X are similar to those in earlier operating systems but offer options unique to Apple's new operating system.

Spend a few minutes at your computer exploring contextual menus and you may find yourself working a little more efficiently.

E-ASIA digital library

New Online Library Resource Offers Round-the-Clock Study, Research Opportunities

The Knight Library's East Asian Bibliographer Bob Felsing has created a new online library resource designed to contribute to the research and scholarship of East Asia.

The E-Asia Digital Library (**http://e-asia.uoregon.edu/**) is a collection of searchable full-text e-books and audio files, images, and map holdings pertaining to the history and culture of East Asia. In addition to resources from the UO Library's Special Collections, E-Asia resource materials include the contributions of various individuals and organizations.

Non-Administrative Access to OpenVMS on Oregon to Phase Out by Fall 2004

Joe St Sauver, Ph.D.
Director, User Services and Network Applications
joe@oregon.uoregon.edu

OpenVMS has been a wonderful operating system for UO's academic user community for fifteen years, but the time has come for the university to begin phasing out OpenVMS as a general-purpose academic computing platform. We will be doing so over so over the next two years, with all academic user access to OpenVMS on **oregon.uoregon.edu** scheduled to conclude by fall 2004.

In future issues of *Computing News* we will provide detailed transition information, but at this time we at least want to give you an overview of what will be involved in decommissioning OpenVMS on **oregon.uoregon.edu**, and advance notice of what's coming.

Daisy and Donald users not affected. Please note that the following information pertains only to academic users working on **oregon.uoregon.edu**, and does not affect any administrative computing users working on **daisy.uoregon.edu** or **donald.uoregon.edu**.

Also note that the phase-out described here will be taking place over a *two year* period. We are informing you of these plans early and will work with all current Oregon users to ensure the transition is as smooth as possible.

Accounts

No new accounts will be created on **oregon.uoregon.edu** at this time. Any requests for exceptions to this policy will be closely scrutinized and will require compelling justification. (We are taking this step now to ensure that if you aren't currently using Oregon, you don't get started on the wrong path, given our announced plans.)

Email

We recognize that most folks who currently use **oregon.uoregon.edu** use it for email, and typically connect via POP3 or IMAP using a desktop client such as Eudora. For those users, our recommendation is to gradually transfer their email to Darkwing (in the case of faculty, staff and graduate students), or to Gladstone (in the case of undergraduate students who are currently on Oregon).

You'll find information on migrating saved Oregon email messages to Darkwing or Gladstone in the "Migrating Mail…" article on page 15. Disk quotas on Darkwing will be adjusted on request to accommodate mail currently stored on Oregon.

In the fall of 2004, any email still being sent to Oregon will automatically be redirected to Darkwing.

Web pages

We also recognize that in addition to email, some of you may have web pages on Oregon. In general, you should be able to easily move most of those web pages to Darkwing or Gladstone without any trouble—other than having to do the work involved in physically transferring the files and adjusting the URL of any page referring to **www-vms.uoregon.edu** or **oregon.uoregon.edu**

Again, if a quota increase is required to facilitate the movement of those web pages from **oregon.uoregon.edu** to Darkwing or Gladstone, it will be routinely made.

Users Running Applications Other than Email and Web Pages from Oregon:

If you're using applications other than email or web pages on Oregon, we urge you to contact *consult@oregon.uoregon.edu* and arrange to move your applications to Darkwing or Gladstone in a timely fashion. Yes, it is true we will still support **oregon.uoregon.edu** for another two years. However, we have limited staff to help you migrate your current OpenVMS applications, and if you wait until late summer 2004, we can't guarantee that we'll have sufficient time to devote to your particular application.

Why Now?

We know that many of you are interested in knowing why we're announcing this transition at this time. There are a variety of factors, including:

- **VMS support staff attrition.** A key member of our VMS Systems support staff is scheduled to retire within the year, and it is not clear that we'll find a suitable replacement. Unless that position is refilled, we'd be left with less than 1.0 FTE worth of VMS systems support staff for both academic and administrative OpenVMS support. That simply isn't enough to adequately support and maintain mission-critical OpenVMS systems, considering the need to provide coverage during vacation time, sick time, business-related travel, and so forth.

- **Administrative Computing is examining alternatives.** Academic access to OpenVMS has always been predicated on Administrative Computing's continued commitment to this system. This is largely due to Academic Computing's historical pattern of "inheriting" hand-me-down AlphaServers when Administrative Computing systems get upgraded, as well as a history of shared system support (whereby Academic Computing OpenVMS systems are handled incidental to Administrative Computing requirements). If Administrative Computing drops its commitment to OpenVMS, Academic Computing would be hard-pressed to fund the required hardware and staff to sustain that operating system.

OpenVMS Phase-Out, continued…

- **Hardware support.** OpenVMS has traditionally run on Digital (then Compaq and now HP) Alpha hardware. HP has indicated that sales of AlphaServer hardware will last until at least 2006, with migration to HP Itanium-based servers. Unfortunately, sales of Itanium or Itanium 2-based servers have been slow, with less than 1000 Itanium-based servers shipping in Q2 2002, and no commitment to that chipset as yet from Dell, a key industry trend-setter (see **http://zdnet.com.com/2100-1103-955962.html** and **http://www.pcworld.com/news/article/0,aid,102470,00.asp**).

Moreover, it will be difficult for OpenVMS, shipping on a limited range of proprietary hardware, to remain competitive with open source operating systems (such as Linux) running on commodity mass market Intel hardware (such as multiprocessor Xeon-based systems).

- Operating system support. OpenVMS was created by Digital Equipment Corporation. Compaq acquired Digital Equipment Corporation, and OpenVMS, in June 1998. In turn, Compaq merged with HP this past summer. HP's best current public information about its plans for the OpenVMS product line is available at

http://www.openvms.compaq.com/openvms/roadmap/openvms_roadmaps_files/OPENVMS_ROADMAPS.PPT

(Note that the support futures outlined in that document do *not* represent a contractual commitment on the part of HP, and are subject to change without notice.)

In its discussion of OpenVMS's future (**http://www.hp.com/hpinfo/newsroom/press/07may02b.htm)**, HP strongly signals that HP-UX is HP's preferred direction for its customers. (On the other hand, see **http://www.compaq.com/hps/commitment.html**, which appears to express a strong commitment to OpenVMS.)

- Third Party Network Software support. The UO has relied on third party commercial network software to connect **oregon.uoregon.edu** to UOnet and the Internet at large. We have recently encountered a variety of issues in this area of network software support, including problems with SSH v.2, IPv6, and spam management measures. These and other problems convince us that OpenVMS will be increasingly hard to work with in a intensely networked environment like the UO's.

- Application support. It's increasingly difficult to get commercial software product support for OpenVMS. For example, Mathematica Version 4.2 isn't available for OpenVMS, and in fact the latest version of Mathematica that we've been able to obtain for OpenVMS has been 2.2. Likewise, the latest version of SPSS is 11.5, but the latest version of SPSS that we've been able to obtain for OpenVMS is 7.3. Other software applications (with the notable exception of SAS) also tend to be low priority for vendors—with OpenVMS support lagging if it's available at all.

Yet another example of the demise of OpenVMS applications can be seen in Captaris' September 12th, 2002, end-of-life announcement for the WebMail product we've been running for OpenVMS users. For details, see **http://www.captaris.com/staticresources/html/infiniteeol/wmiceol.html** (Please note that IMHO web email, aka "green" web email, as normally used in conjunction with Darkwing and Gladstone, is *not* affected in any way by Captaris' announcement concerning their product. IMHO web email is a completely different product, and continues to be the recommended way for casual users to access their Darkwing and Gladstone email via the web.)

- Other sites have migrated, or are in the process of migrating from OpenVMS to alternative platforms. Most government labs moved away from OpenVMS as a scientific computing platform in the mid- to-late 1990s, as have most colleges and universities.

In conclusion, while OpenVMS has done a great job for UO users for a long time, it is time for OpenVMS to enjoy a well-deserved retirement at the University of Oregon. If you have any comments, questions or concerns about this announcement, please feel free to contact me at

Darkwing Email Addresses Simplified

Traditionally, all UO email addresses have included the actual name of a machine (such as Darkwing, Gladstone or Oregon).

Due to a recent change, however, Darkwing users can now omit "darkwing" from their email addresses. This means, for example, that if your email address was formerly *jsmith@darkwing.uoregon.edu* you can now tell your correspondents to send email to *jsmith@uoregon.edu* instead.

In addition to shortening and simplifying your email address on Darkwing, many users may also find that an email address simply ending in *@uoregon.edu* (rather than *darkwing.uoregon.edu*) may convey a more professional or official appearance.

To ensure that mailing list subscriptions aren't disrupted, all email sent outbound from Darkwing will continue to be written by default as coming from "darkwing.uoregon.edu" unless you manually change your email address in your email client's options/settings/preferences.

Please also note that this change affects *only* Darkwing (Gladstone and Oregon users are not affected)—and only darkwing email. Web pages hosted on Darkwing, for example, should still have URLs referring to darkwing.uoregon.edu (see the article "Watch URL Syntax…" on the bottom of page 22) . Likewise, when using your Darkwing account to authenticate on the UO modem pool or wireless network, continue to specify *username@darkwing.uoregon.edu*

Migrating Mail from OREGON (OpenVMS) to DARKWING or GLADSTONE (UNIX)

Lucy Lynch
User Support Specialist
llynch@darkwing.uoregon.edu

Did you know you can transfer your existing mail from Oregon (VMS) to a new or existing Unix account on Darkwing or Gladstone? This process uses IMAP (Internet Message Access Protocol) to make the transfer and leaves the source mail on VMS. If you want to use this transfer method, you'll need the following before you start:

- an SSH client so you can log into Oregon and your Unix account
- Your username (i.e. *johndoe)* and password for both accounts
- the hostname for your Unix account (i.e., **darkwing.uoregon.edu** or **gladstone.uoregon.edu**)

Now, follow the steps below to transfer your Oregon mail to either a new or existing Unix account:

Moving Mail to a New Unix Account

Step One: Log in on Oregon (VMS) using SSH and type the following commands:

```
$ migrate -batch -toprefix "mail/"
From which host: oregon.uoregon.edu
Username on oregon.uoregon.edu: johndoe
Password for johndoe on oregon.uoregon.edu: xxxxxx
To which host: darkwing.uoregon.edu
Username on darkwing.uoregon.edu: johndoe
Password for johndoe on darkwing.uoregon.edu: xxxxxx
some# messages moved ...
```

(This example will migrate email for the username *johndoe* from Oregon to the hostname **darkwing.uoregon.edu** and store it the mail subdirectory.)

Step Two: Next, log into your new Darkwing or Gladstone (Unix) account using SSH and type:

```
% ls -al .mail
```

If you see a message like this:

```
.mail: No such file or directory
```

then type:

```
% mv mail/INBOX .mail
```

If you see a message similar to this:

```
-rw-------  1 llynch  cc_prod  1659  Sep 27  13:07  .mail
```

STOP! You need to use the process for an existing account.

Moving Mail to an Active Unix Account with an Existing Mail Directory:

Step One: Log into your Unix (Darkwing or Gladstone) account and type:

```
% mkdir oldmail
```

Step Two: Log into Oregon using SSH and move mail to oldmail, as follows:

```
$ migrate -batch -toprefix "oldmail/"
From which host: oregon.uoregon.edu
Username on oregon.uoregon.edu: johndoe
Password for johndoe on oregon.uoregon.edu: xxxxxx
To which host: darkwing.uoregon.edu
Username on darkwing.uoregon.edu: johndoe
Password for johndoe on darkwing.uoregon.edu: xxxxxx
some# messages moved ...
```

Step Three: Log back into your Unix account using SSH and move your Oregon INBOX to the mail directory by typing:

```
% mv ~/oldmail/INBOX ~/mail/vms-mail
```

Additional Considerations: If you have additional oldmail that you want to move to your current mail directory, first type **`% ls -al oldmail`** You'll see something like this:

```
23% ls -al oldmail
total 50
drwxr-xr-x  2 llynch  cc_acad   512 Sep 3 14:12 ./
drwxr-xr-x 34 llynch  cc_prod   8192 Sep 3 14:12 ../
-rw-------  1 llynch  cc_acad   1124 Sep 3 14:11 MAIL
-rw-------  1 llynch  cc_acad   508 Sep 3 14:11 sent-mail
-rw-------  1 llynch  cc_acad  997 Sep 3 14:12 sent-mail-mar-2002
```

Issue the following command to move files as needed, renaming those that may conflict with existing files in your Unix mail directory (typing **ls -al mail** will show the files in your mail directory):

```
% mv ~/oldmail/sentmail ~/mail/vms-sentmail
```

Forwarding your Oregon account: Once you've moved your mail, you'll want to set a forward on Oregon so that any new messages sent to your Oregon account automatically arrive in your Unix mailbox (see References below).

Note: *Be sure to delete old mail on Oregon when you're positive everything has been moved successfully.*

References:

For more details on forwarding your mail, go to **http://darkwing.uoregon.edu/~cchome/mailforward.html**

To learn more about the migrate utility, see **http://oregon.uoregon.edu:7633/doc/user_vms/book_u5.html#pmdf_migrate_utility**

To view MAN pages for Unix commands (**ls**, **mv**, etc.), see **http://darkwing.uoregon.edu/~llynch/cgi-bin/man.cgi**

CHECK OUT THE NEW, IMPROVED UO LIBRARY WEBSITE:

http://www.libweb.uoregon.edu/

Intrusion Detection Tools Play

Network data analysis tools like Snort provide a window into the world of the hacker

John Kemp
Senior Security Engineer
kemp@ns.uoregon.edu

The Security Group at the University of Oregon performs a variety of services in the area of computer and network security. Among these services are general security consulting, risk assessment, vulnerability scanning, incident handling, and intrusion detection. The latter—intrusion detection—is among the most interesting of these because it provides a direct window into the world of the hacker.

To help safeguard a network, various types of Intrusion Detection Systems (IDSs) can be employed, and they can be used in many ways. IDSs can be divided into two broad categories: host-based systems and network-based systems.

Host-based detection involves running software on a host to monitor just that particular host at a high level of detail. Network-based systems are placed strategically within a network to passively listen to a large percentage of an organization's network traffic.

Network-based systems may not provide the precision or level of detail that a host-based system can, but they do have the advantage of being centralized, and they can yield significant returns for a smaller overall investment. The rest of this article focuses on network-based systems.

IDSs can be used for tasks as simple as network traffic accounting or as complex as detecting anomalous behavior in network traffic. One of their more common uses is to monitor the network for incoming attacks. IDSs utilize a database of signatures that describe what the network traffic "looks like" for certain well known attack programs. Detection of things like the "Code Red" and "Nimda" network worms are common. IDSs can also be used to detect port scanning or Denial-of-Service (DoS) attacks, where a flood of traffic is sent in an attempt overload a system on the network.

The more quickly a break-in is detected and dealt with, the better. Most IDS systems have near-real-time capabilities for detection and notification. Once an attack is detected, a range of actions may follow. The first course of action is to notify the attacker's Internet Service Provider (ISP) and request that the attacker be removed from the network. Local network engineers can respond by putting filters in place to block further attacks from the same source. In cases where break-in attempts are successful, campus administrators are notified and the affected machines are removed from the network until the damage can be cleaned up.

It should be emphasized that there is less value in detection than there is in prevention. It is much better if an attack is prevented before it occurs, rather than detected after it has been successful. For this reason, security professionals usually recommend that resources be committed to preventative measures (such as installing firewalls and keeping up-to-date on application and operating system patches) before they're expended on detection. A break-in itself, and the cleanup afterwards, are costly events. Nevertheless, an IDS is still a valuable tool for detecting attacks and break-ins, and monitoring anomalous behavior on a network.

It is much better if an attack is prevented before it occurs, but an IDS is still a valuable tool for detecting break-ins and monitoring anomalous behavior on a network

Software for running network-based IDSs is available in the form of commercial and open-source applications. Some of the more popular applications are Snort, ISS RealSecure, Bro, Cisco NetRanger, and Network Flight Recorder. Snort and Bro are both open-source, and are freely available. What follows is a more detailed discussion of Snort as a sample case of a network-based IDS.

How Snort Works

Snort is a network data analysis tool that can be run on Unix and Windows systems. As the name implies, Snort was originally designed as a packet sniffer. It evolved into a more sophisticated tool after Martin Roesch of Sourcefire, Inc., who was trying to design a better version of tcpdump for displaying packet dumps, realized he could easily extend his new sniffer's capabilities to do pattern matching. And so Snort turned into a rudimentary network IDS as well. Since then, a great deal of work has been done to expand the functionality of the program.

Snort can be run in three different modes: as a packet sniffer, a packet logger, or an IDS.

1. Packet sniffing mode. The simplest mode is running Snort from the command line of a Unix system in much the same way as tcpdump.

For example, to look at the internal traffic on a Unix system, you'd issue the command

```
# snort -dave -i lo
```

Important Role in Network Safety

The display format is like tcpdump, but it is displayed in a much more readable format. In addition, an ASCII representation of the data is displayed alongside the hexadecimal packet data.

2. Packet logger mode. Snort can also be run in packet logger mode. In this mode, Snort will save the packet data to a disk instead of displaying it to the screen. The default filename format is **snort-<MMDD@HHmm>.log**, where MM=month, DD=day, HH=hour, and mm=minute, which indicates the time that logfile was created. In the following example the data is saved in binary format, and the file is created in the directory **/var/log/snort**:

```
# snort -i eth0 -b -l /var/log/snort
```

Without the binary flag, snort will split out the data into directories based on the IP address of the remote machines, and within those directories it will save individual files, based on protocol and port number, containing the fully formatted ASCII data of the packets. While this can create a large number of files and a significant amount of data on a busy system, it is a logical way for storing this kind of data.

3. IDS mode. The full capabilities of Snort come into play when it is run as an IDS system. Snort has preprocessing, signature matching rules, advanced logging, and alerting capabilities when run in IDS mode. A configuration file can be used to describe these extended features. This is the default mode that Snort will try to run in, but it is common to specify this mode explicitly on the command line:

```
# snort -c snort.conf -l /var/log/snort -b -A fast
```

The above command tells snort to read from the configuration file **snort.conf**, to log to the directory **/var/log/snort**, to save the data files in binary format, and to send brief alerts when an intrusion is detected. For later analysis the files can be read back in using the **-r read** option to Snort.

The most common use of Snort is as a signature-based IDS. A signature database is created that contains identifying features that occur in the network packet data from known attacks. Over time, as more attacks are discovered and captured, the signature database is expanded. The community of Snort users is large, and a community database of the signatures of well-known attacks is maintained at the Snort website.

When an attack is detected, it can be logged, or trigger an alert. The alert mechanism in Snort is very flexible. Alerts can be sent as brief headers or as full text. Alerts can be transmitted using the syslog mechanism, or via SMB message popups, or passed over a network socket to another system. Additional alert options are available for storing alert messages into databases.

The signatures detected by Snort are described by a rules language. These rules contain an action, a protocol field, source address and source port, destination address and destination port, traffic direction, and an options field that is used to match the specific contents of packets. Here is one example:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:
"NETBIOS nimda .eml"; content: "|00|E|00|M|00|L";
flags:A+; classtype:bad-unknown; reference:
url,www.datafellow s.com/v-descs/nimda.shtml;
sid:1293; rev:2;)
```

This rule represents a check for one variant of the Nimda worm. The source and destination are defined by variables that classify the traffic as coming from a remote network to the local network. The message section is used to define an informative message to send when issuing the alert. In this case, a NetBIOS-over-TCP packet coming into the network on port 139, that contains the string **<null>E<null>M<null>L**, would trigger an alarm. A reference link to information about the vulnerability can be included as a part of the alert.

Here is another example of a Snort rule. In this case, a specific set of web servers is being watched for Code Red attempts, and the attack is coming into the network on port 80. Instead of the plain "content" type, uricontent type is used so that the rule will match only in the event that the string **"scripts/root.exe?"** is found within the section of the packet that contains an HTTP request:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS
80 (msg:"WEB-IIS Code Red v2 root.exe access";
flags: A+; uricontent:"scripts/root.exe?"; nocase;
classtype:web-application-attack; reference:
url,www.cert.org/advisories/CA-2001-19.html;
sid:1256; rev:3;)
```

Some of the more powerful features of Snort are available in IDS mode through preprocessor modules. These modules operate on streams of data that are gathered together and organized, rather than on individual packets. For certain types of attacks, this sort of buffering of the data is necessary. Things like HTTP decoding, port scan detection, telnet stream scanning, and defragmentation can be performed using these modules.

Protect Your Server

The kinds of attacks that are appearing on UOnet are about what you might expect. There are typically 10 to 20 scans every day covering the entire UOnet address space. WWW server and FTP server buffer overflow attacks are common. Interestingly enough, Microsoft SQL Server is also a popular target. Less common but still popular are buffer overflow attacks against Unix machines. Probes looking for RPC services, older SSH versions, and LPD vulnerabilities are common.

Intrusion Detection Tools, continued...

Stay current. The best advice in these cases is to make sure that your server software is up-to-date, especially your WWW, FTP, and SSH server software. If your server software is not kept current, the odds are very good that your system will be compromised.

Use Windows File Sharing with care. Break-in attempts against Windows machines that have Windows File Sharing enabled have also been common. Shares that have weak passwords, or that have blank passwords, have been hardest hit. In other cases, vulnerabilities in the File Sharing authentication mechanism have been targeted.

Run antivirus software. If you are not using Windows File Sharing, make sure it is disabled. The recent implementation of a packet-filtering policy on campus, which blocks non-affiliated users from accessing Windows File Sharing, has been effective in blocking most of these types of attacks. Nevertheless, email viruses continue to be successful, taking advantage of the fact that Microsoft Outlook is a common mail client, and that many users do not have anti-virus software running on their machines. Running anti-virus software on a Windows machine and keeping it up to date is a simple way to guard against many of these attacks.

Important Note on Acceptable Use

Please note that running a sniffer on your machine can be an invasion of privacy and a violation of the acceptable use policies for the UOnet network. In general, you should run Snort only on a machine that is wholly operated by you and where you are the only user on the machine. Additionally, you should only observe traffic that involves your own machine.

Restricting the traffic that Snort observes can be done either by specifying the loopback interface or by specifying the local hostname as an argument to the "host" option. Specifying the loopback interface makes Snort only look at traffic that involves the machine communicating internally with itself. Specifying the "host <myhostname>" option makes Snort only look at traffic to and from the local machine.

When run in either of these ways, Snort can be a helpful tool for understanding Internet protocols and the behavior of Internet traffic. All other uses should be considered forbidden, except where permission is explicitly granted for problem resolution under the direction of Network Services.

References:

SANS Reading Room
http://rr.sans.org/intrusion/intrusion_list.php

CERT Advisories
http://www.cert.org/

Snort Documentation and IDS References
http://www.snort.org/docs/

The MicroHelp Security Pages
http://micro.uoregon.edu/security/

The MicroHelp Norton Anti-Virus Distribution
http://micro.uoregon.edu/av/nav.html

The UO Security Group
http://security.uoregon.edu/

Network Services Blocks SMB Traffic from Off-Campus

Because of the potential for remote attackers exploiting a vulnerability in Windows NT/2000/XP Server Message Block (SMB) protocol (re: "...More Microsoft Security Loopholes" on page 24), Network Services has installed filters on the UO network that effectively block SMB traffic from off-campus.

Before the block, PC systems that were not adequately secured (e.g., unpatched systems, or systems with poor or nonexistent password protection) were vulnerable to being compromised or disabled by attacks from off-campus. Now, such systems are vulnerable only from attack by on-campus systems.

If you need to use Windows File Sharing or other SMB services, you can access them by using our encrypted VPN (Virtual Private Network) software. For VPN software download links and documentation, see **http://micro.uoregon.edu/getconnected/**

Protect Yourself

As always, we recommend that you routinely run Windows Update to keep your system patched with all critical updates. You should also secure your machine by password-protecting all accounts that can be accessed remotely.

Questions?

If you have any questions about securing your PC or using VPN, or are unsure how the SMB filter may affect you, please contact *nethelp@ns.uoregon.edu* or call Network Services at **346-4395**.

To learn more about VPN at the UO, see the Spring 2002 *Computing News* article, "VPN Services Now Available" (**http://cc.uoregon.edu/cnews/spring2002/vpn.html**).

Open Proxy Servers: A Growing Source of Spam

Joe St Sauver, Ph.D.
Director, User Services and Network Applications
joe@oregon.uoregon.edu

Most of the spam sent to UO users comes from one of five sources:

1. So-called "bulletproof" email servers (run by dedicated spam houses and connected by ISPs who fail to enforce any acceptable use policy on their customers)

2. Throw-away free email accounts which get used until they're cancelled, at which point spammers create and abuse new throw-away email accounts

3. Open SMTP relays, e.g., hosts that are willing to accept and resend email for virtually anyone, including random spammers

4. Abusable form-mail cgi-bins. These are web pages that are intended to be used just to send comments to a particular address, but which can be "hijacked" to send email to random addresses of a spammer's choice

5. Open proxy servers (systems that will accept connections from any network address, acting as a blind intermediary to virtually any other network addresses).

It is this last category—spam from open proxy servers—that has become a growing concern for Darkwing, Gladstone, and Oregon users lately.

In an effort to deal with this problem, the Computing Center Systems group—the group that's ultimately responsible for administering Darkwing, Gladstone, and Oregon's anti-spam measures—has been experimenting with a DNS-based Open Proxy blacklist known as the Blitzed Open Proxy Monitor. In a nutshell, when an email is received from network address A.B.C.D, the mail server checks via the domain name system to see whether or not the address D.C.B.A.opm.blitzed.org is defined. If it is, this signals that mail from that address is coming from an open proxy server, and we reject that email.

This check augments, but does not replace, other anti-spam measures already in place on the university's large shared hosts, including use of the mail-abuse.org RBL+ service.

We are also evaluating other open proxy black lists, including the monkeys.com Open Proxy List (**http://www.monkeys.com/anti-spam/filtering/proxies.html**) and the Osirusoft Open Proxy List (**http://relays.osirusoft.com/faq.html**).

Like the Blitzed OPM, checking the monkeys.com list or the Osirusoft list is simply a matter of querying DNS to see whether or not D.C.B.A.proxies.relays.monkeys.com or D.C.B.A.relays.osirusoft.com are defined for a given numerical network address.

As open proxies are used to send email to Darkwing, Gladstone or Oregon users, they're being added to **http://darkwing.uoregon.edu/~joe/open-proxies-used-to-send-spam.html**, a page which tracks not only the source of open proxy spam, but also identifies which of the open proxy lists knows about each of those open proxy servers.

Based on these efforts, we hope to dramatically reduce spam received from open proxy servers, much as we've been able to successfully reduce other sources of spam abusing UO email addresses.

What's New on the VMScluster…

New VMS Manual Sets Online

Last August, the VMScluster was upgraded to VMS 7.3, and its C compiler, to v. 6.5.

Release notes for the new version of VMS are available at **http://web-vms.uoregon.edu/vms_doc/v73/6637/6637PRO.html** and the complete manual set is online at **http://web-vms.uoregon.edu/vms_doc/index.html**

To see a summary of new features, go to **http://web-vms.uoregon.edu/vms_doc/v73/6620/6620PRO.html**

For a complete manual set on v 6.5 of the C compiler, see **http://web-vms.uoregon.edu/vms_help/cc$alpha_help_065/index.htm**

See the **Release Notes** for information about the changes and enhancements in the new version. If you want to use the old version, see Section 8.

Need help? Go to **http://web-vms.uoregon.edu/vms_help/cc$help.html**

HITMAN Limits on VMScluster

Because abandoned interactive sessions unnecessarily tie up system resources and pose a security risk, we use a utility called HITMAN to kill sessions that remain idle for longer than a prescribed time. The maximum settings for idle time settings are shown below:

Start-end times	Maximum idle time
OREGON:	
7 AM - 6 PM	600 minutes
6 PM - 11PM	120 minutes
11 PM - 7AM	60 minutes
DONALD, DAISY:	
7 AM - 6 PM	60 minutes
6 PM - 11PM	120 minutes
11 PM - 7AM	60 minutes

In the past, some SSH sessions were protected from termination due to the type of terminal device (FTA) associated with their processes. This aberration has now been eliminated, so be aware that all your SSH sessions are also subject to HITMAN limits.

Networking Notes…

UO Increases Internet Transit to 51Mbps

Thanks to recent price reductions from NERO (Network for Education and Research in Oregon), the UO is able to more than double the bandwidth rate limit for UOnet (up from 21Mbps to 51Mbps). This means you can expect less congestion at peak usage times.

The UO's participation in The Quilt (**http://www.thequilt.net/**), a project of Internet2, is a large contributing factor in the lower costs available to NERO for Internet Transit bandwidth.

For more information on NERO, see **http://www.nero.net/**

Graphical AS Path Visualizer

If you'd like to see how Internet traffic travels from point to point on autonomous systems (AS), go to **http://zebra.swinog.ch/sysctl/gasp/index.php** Enter the IP address of the network you're examining, and you'll see a screen showing a graphical representation of its path. To get more details about a particular AS, click on the icon representing each collection of routers.

NANOG, ARIN Hold Joint Meeting in Eugene

Under the auspices of the University of Oregon and Sprint Corporation, ARIN (The American Registry for Internet Numbers) and NANOG (the North American Network Operators Group) are holding their first joint meeting at the Eugene Hilton and Conference Center this fall.

NANOG is a forum for coordination of network operations in North America comprising senior engineering staff from tier 1 and tier 2 Internet service providers.

ARIN is a nonprofit corporation that administrates the registration of Internet Protocol (IP) numbers for North America, South America, the Caribbean, and sub-Saharan Africa.

The event, which runs from October 27 through November 1, will give network operators a great opportunity to participate in ARIN policy discussions. For details, see **http://www.nanog.org/arin.html** and **http://www.nanog.org/mtg-0210/**

MPEG-4 Licensing Fees Capped

Last July, definitive licensing terms and pricing schedules were set for MPEG-4, a protocol for Internet interactive multimedia.

Although licensing fees are capped at $1 million a year, there are higher charges for cable TV and stored video applications, including per-minute charges for Internet viewers.

For more on the new licensing terms and their possible implications, see **http://theregus.com/content/6/25623.html** ("MPEG 4 is Go…") and **http://www.macworld.co.uk/news/main_news.cfm?NewsID=4956** ("MPEG licensing resolved").

Oregon's Commercial Fiber Upgrade Schedule Online

Track the state's progress at

http://www.econ.state.or.us/telecom/deploysched.htm

UO, Oregon Gigapop, NYSERNet Set IPv6 Land Speed Record

The UO Computing Center was part of a team that set the first record for Internet performance using IPv6, the next-generation Internet protocol in the Internet2 Land Speed Record Competition this September. Collaborating with NYSERNet, a New York based nonprofit networking organization, as well as the staff of Abilene, the Indiana network operations center, and the Internet2 End-to-End Performance Initiative, the UO transferred 3.47 gigabytes via the Oregon Gigapop over 3000 miles from Eugene, Oregon, to Syracuse, New York, at a speed of 39.81 terabit meters per second.

Other Internet2 sites utilizing IPv6 are shown in the table at right.

INTERNET2 SITES Utilizing IPv6

IPv6 Native Gigapops	IPv6 Native Peer Networks/Exchanges	IPv6 Native Internet2 Router Nodes
Indiana Gigapop	6TAP	Atlanta
NYserNet	CUDI	Cleveland
Pittsburgh Gigapop	SURFNET	Chicago
Great Plains Network	APAN/TransPAC	Denver
WISCnet	SingAREN	Houston
MAX	JGNv6/WIDE	Indianapolis
Oregon Gigapop	vBNS+	Kansas City
SDSC		Los Angeles
FRGP		MIX
NOX		New York City
ONEnet		Seatlle
		Sunnyvale
		Washington DC

References:

Internet2:
http://www.internet2.edu/
NYSERNet:
http://www.nysernet.org/
I2 Land Speed Competition:
http://www.internet2.edu/lsr/
Oregon Gigapop:
http://www.ogig.net

ICANN Moves to Improve Accuracy of Whois Data

On September 3, ICANN (the Internet Corporation for Assigned Names and Numbers), which manages the Internet's global addressing system, announced that it is taking steps to improve the accuracy of the "Whois" database of Internet addresses.

First on ICANN's list is improving its facilities for handling reports from the public about incomplete or inaccurate Whois data. It has also taken steps to enforce its contracts with domain name registrars, who are legally bound to provide complete and accurate data to the ICANN registry.

In particular, ICANN has cracked down on VeriSign, the world's largest retailer of top-level Internet addresses. VeriSign is charged with being consistently negligent in meeting its contractual obligations to provide accurate Whois information, and is now threatened with revocation of its right to sell top-level domain names if it fails to rectify violations .
See "ICANN Threatens to Revoke VeriSign's Right to Sell Dot-Com Names" at

http://www.washingtonpost.com/ac2/wp-dyn/A33395-2002Sep3

Where to Report Whois Data Problems

To report inaccuracies in the database, go to
http://www.internic.net/cgi/rpt_whois/rpt.cgi

Track Network Info with RWhois

If you're tracking down a spammer or an unreachable web address, or seeking information about a particular domain, you'll find the RWhois directory service protocol a useful tool.

A project run by Network Solutions, Inc., the RWhois database streamlines the process of researching domain names, networks, and IP addresses. To learn more about RWhois, go to **http://www.rwhois.net/**

Free Multicast ISP List Service

As a service to the community, Multicast Technologies, Inc., maintains a site for multicast service providers to list their service offerings at **http://www.multicast-isp-list.com/**

P2P Filesharing Can Blow Bandwidth

Recent traffic measuring research indicates that peer-to-peer (P2P) filesharing eats up bandwidth and costs Internet service providers and subscribers big-time.

In "How to blow your bandwidth," published September 6 on **gobleandmail.com**, Jack Kapica describes how even modest use of P2P—such as searching for and downloading a few songs from Kazaa or Morpheus—can push subscribers over their commercial ISP's monthly download limit in no time.

For more details on P2P's bandwidth consumption, see

http://rtnews.globetechnology.com/servlet/ArticleNews/tech/RTGAM/20020906/gtcybsept6/Technology/techBN/

To read the full white paper on P2P traffic, see "The Effects of P2P on Service Provider Networks" at

http://www.sandvine.com/register.asp?TID=1&ID=1

This report is also available at Forbes.com (**http://itresearch.forbes.com/**)

Cisco 675 DSL Customers Should Upgrade their CBOS to 2.4.6

Joe St Sauver, Ph.D.
Director, User Services and Network Applications
joe@oregon.uoregon.edu

On May 23, Cisco issued a security advisory for users of Cisco 600 DSL routers, including Cisco 675s and Cisco 678s (DSL routers commonly used by Qwest-connected DSL customers here in the Eugene-Springfield area). Details about that security advisory are available at: **http://www.cisco.com/warp/public/707/CBOS-DoS.shtml**

If you are a Qwest DSL customer and have a Cisco 675 or Cisco 678 and you are not running CBOS 2.4.6, please see **http://www.qwest.com/dsl/customerservice/ciscosecurityadvisory/index.html** for information on how to download and install the updated firmware for your DSL router.

Spam Remedies: Some Special Federal

You can report certain kinds of spam directly to the appropriate government agency

Joe St Sauver, Ph.D.
Director, User Services and Network Applications
joe@oregon.uoregon.edu

By now, most UO faculty, students and staff know they're encouraged to report spam they may receive on Darkwing, Gladstone, or Oregon to *spam@uoregon.edu* Once we receive a report, we can file complaints or tweak our local filters to block chronic spam sources. (As always, when you forward spam to us, please be sure it has full, "verbose" headers and was received within the last day or so, otherwise we may be unable to help.)

Aside from routine, nuisance spam, you may also receive some unsolicited email that's of special interest to federal regulatory or law enforcement agencies. In that event, you may report it directly to the appropriate agency, as described below:

Investment/Securities Scams

The SEC's Office of Internet Enforcement Complaint Center (**http://www.sec.gov/complaint.shtml**) indicates that investment-related scam spam can be forwarded to *enforcement@sec.gov* To see examples of the sort of litigation the SEC has brought against parties engaging in Internet-related securities manipulation, go to **http://www.sec.gov/divisions/enforce/internetenforce/litreleases.shtml**

Attempts to Unlawfully Sell Prescription Medications Online

If people attempt to sell you prescription medications online without requiring a physician's prescription, the Food and Drug Administration would like to know about it. You can report emails promoting illegal medical products by forwarding those emails to *webcomplaints@ora.fda.gov* (see **http://www.fda.gov/oc/buyonline/buyonlineform.htm**).

US Customs Service CyberSmuggling Center, Child Exploitation Unit

Occasionally you may receive spam related to child pornography. As noted at **http://www.customs.ustreas.gov/enforcem/child.htm** you should immediately report this to the US Customs Service at **1-800-BE-ALERT** or the National Center for Missing and Exploited Children at **1-800-843-5678**, or contact the Customs Service CyberSmuggling Center at *C3@customs.treas.gov* (see **http://www.customs.ustreas.gov/enforcem/cyber.htm**).

Please note that you should *not* download any child pornographic materials under any circumstances, since the mere possession of this type of material is a violation of federal and state laws. Let trained law enforcement officers conduct their own investigation when it comes to child porn spam.

Internet Fraud in General

Internet fraud complaints may be filed with the FBI's Internet Fraud Complaint Center (IFCC) at **http://www1.ifccfbi.gov/** The IFCC is particularly active in the area of online auction fraud, but it also handles a variety of other Internet-related fraud.

4-1-9 Nigerian Advance Fee Fraud Spam

This type of scam spam, in which overseas, often Nigerian, con men typically offer you a share in millions of dollars worth of "over-invoiced contracts" (if only you will "temporarily" cover the cost of some "advance fees") can be reported to the United States Secret Service by faxing a copy of the 4-1-9 solicitation to **(202) 406-5031**, as noted at **http://www.secretservice.gov/alert419.shtml**

The Secret Service also has jurisdiction over online credit card fraud, among other scams.

Pyramid Schemes or Chain Letters Using the U.S. Mail

If you receive spam that's a pyramid or chain-letter scheme and it uses the United States mail at any step along the way

Watch URL Syntax for Darkwing

Some day, certain virtual hosts such as www.uoregon.edu may be carved off from Darkwing proper and placed on a second machine.

To prepare for this eventuality, it's important that you pay attention to your URL syntax. If you're creating web pages under a public_html directory on Darkwing, be sure to use **darkwing.uoregon.edu** in your URL instead of a virtual host name such as www.uoregon.edu (e.g., use **http://darkwing.uoregon.edu/~joelja** instead of **http://www.uoregon.edu/~joelja**). This ensures that your address will always be accessible, regardless of what machine changes go on behind the scenes.

We will attempt to contact users whose web pages include URLs pointing at virtual hosts. If you have any questions about constructing your URL, send email to our large system consultants at *consult@darkwing.uoregon.edu*

Government Addresses for Reporting Spam

(for example, if it instructs you to send money to an address via the mail), it is illegal and should be reported to the U.S. Postal Service. As noted at **http://www.usps.com/websites/depart/inspect/chainlet.htm** you should turn over a copy of the chain letter or pyramid scheme advertisement to your local postmaster or nearest postal inspector. The nearest Postal Inspection Service office for Oregonians is:

POSTAL INSPECTION SERVICE
UNITED STATES POSTAL SERVICE
PO BOX 400
SEATTLE WA 98111-4000
Phone : 206-442-6300
Fax : 206-442-6304

Unsolicited Commercial Email (Spam) In General

According to its Consumer Complaint Form site at **https://rn.ftc.gov/dod/wsolcq$.startup?Z_ORG_CODE=PU01** the FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into a secure, online database available to hundreds of civil and criminal law enforcement agencies worldwide.

If you wish to report unsolicited commercial email to the FTC, you should forward that spam to *uce@ftc.gov*

Last spring, *Wired News* writer Joanna Glasner reported in her article, "The Law Is Going After Spam" (see **http://www.wired.com/news/politics/0,1283,51486,00.html**) that over ten million spam messages have been forwarded to *uce@ftc.gov* since the beginning of 1998, with over one million pieces of spam being forwarded in the month of March 2002 alone.

State Agencies and Spam

The Oregon Attorney General's Office indicates that consumers can report email scams to the State Department of Justice Consumer Hotline at *consumerhotline@state.or.us* (see **http://www.doj.state.or.us/fraud_spam.htm**) However, there is no indication what will be done with spam that gets forwarded to that address.

Some states, such as California, have been faulted for establishing spam reporting channels but then failing to follow through. (See "Spam Report: California Stumbles Over the Junk E-Mail Question," at **http://www.ecommercetimes.com/perl/story/13817.html**)

For comparison, you may want to take a look at a couple of other state spam complaint policies at **http://www.wa.gov/ago/junkemail/** (Washington) and **http://www2.state.id.us/ag/consumer/tips/whatisspam.htm** (Idaho)

Pointers to all states with anti-spam laws are available online at **http://www.spamlaws.com/state/index.html**

Reporting Spam Directly to an ISP Spam Source: Get Help from *SpamCop*

If you decide to complain directly to the ISP that's hosting spammers—or is itself the source of spam, *SpamCop* can help you find the right ISP. To get started using this service, go to **http://spamcop.net/**

More Spam in the News...

If you're awash in junk email, it may be a small comfort to know you're not alone. Last August, *BusinessWeek* online reported that by the end of this year, unsolicited bulk email could comprise the majority of message traffic on the Internet.

According to the latest figures, spam traffic is up eight percent from a year ago, and it now makes up 36% of all email traveling over the Internet.

Beyond the annoyance factor, spam hogs bandwidth and hampers productivity. For more details on the growing problem of unsolicited bulk email, see

- "You've got spam, and more spam" by Robert Lemos. CNET News.com
http://news.com.com/2100-1001-955842.html

- "If it's spam, the message is 'delete' by Margaret Kane. CNET News.com
http://msnbc-cnet.com.com/2102-1017-955806.html

- "Europe bans spam" by Tim Richardson. *The Register.* **http://www.theregus.com/content/6/25107.html**

Scam o Rama: the Lighter Side of Internet Fraud Info

For an entertaining exposé of recent 4-1-9 advance fee Internet scams, along with law enforcement news and notes and other scam-related FAQs, visit the Scam o Rama site at **http://www.scamorama.com/**

Heads Up! More Microsoft Security

Make sure you get the fixes for these recently reported flaws

Joyce Winslow
jwins@oregon.uoregon.edu

Over the last three months, additional alerts about potential security vulnerabilities in Microsoft products have been issued from various sources. If you're using any of the Microsoft products cited below, make sure you take the necessary steps to protect yourself.

IE and Office Software

Internet Explorer 5.0/5.5/6 and Office 2000/XP, Money 2002/2003, Project 2002. In previous issues of *Computing News, w*e've described numerous IE vulnerabilities ("Be Alert to Ongoing Microsoft Security Problems" **http://cc.uoregon.edu/cnews/summer2002/ms_holes.html** and "Security Problems Still Plague Microsoft" **http://cc.uoregon.edu/cnews/spring2002/ms_probs.html**).

The latest warnings, first posted by San Francisco programmer Mike Benham last August, cite a newly discovered loophole in handling Microsoft's digital certificates and a problem with the PGP (Pretty Good Privacy) encryption program. Digital certificates and PGP are intended to provide security, but these flaws could allow hackers to gain access to credit card and other sensitive information being transmitted over the Internet. Microsoft also disclosed that, in addition to exposing sensitive user information, these security holes could allow an attacker to use Internet-related parts of Office software to run programs that alter data and wipe out the hard drive.

Microsoft urged users to get the new cumulative patch for Internet Explorer at
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-047.asp

Information and Fixes. For more details on these problems, and links to fixes, see

- "Serious flaw found in Internet Explorer"
http://zdnet.com.com/2102-1105-949506.html

- "Certificate Validation Flaw Could Enable Identity Spoofing (Q328145)" **Microsoft Security Bulletin MS02-050** (this site also provides updated patches for Windows 98/NT 4.0/Me/2000/XT, and will soon have fixes for Mac versions):
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-050.asp

- New cumulative patch for Internet Explorer:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-047.asp

- "Unsafe Functions in Office Web Components (Q328130)" **Microsoft Security Bulletin MS02-044**
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-044.asp

Microsoft Word

A recently disclosed flaw in all versions of Microsoft Word leaves files vulnerable to attackers who could steal computer files by bugging a document with hidden code. Word 97 is most vulnerable, but thus far Microsoft is committed to correcting the problem in later versions only. The Word 97 exploit is especially dangerous because it leaves almost any file—even files on a secure server—vulnerable to theft, and the attacker's "spy" field code can scan for hundreds of files without being detected.

Until the problem is corrected, Microsoft suggests Word users view hidden code in every document they open. For details, see

- "Microsoft Word flaw may allow file theft"
http://www.cnn.com/2002/TECH/ptech/09/13/microsoft.word.bug.ap/index.html

- Microsoft's information page at
http://www.microsoft.com/technet/treeview/default.asp?url=/Technet/security/topics/secword.asp

- Woody's Office Watch article, "The biggest Word 97 Security Hole Yet" at
http://www.woodyswatch.com/office/archtemplate.asp?v7-n42

SMB for Windows NT/2000/XP

The SMB (Server Message Block) protocol, which is used to share files, printers, serial ports, and to communicate between computers using named pipes and mail slots, has an unchecked buffer in a section of code that requests the SMB service. This flaw leaves Windows NT/2000/XP systems vulnerable to being crashed by a denial of service attack.

Information and Fixes. For more information on the SMB flaw, as well as fixes for XP/NT/2000, see **Microsoft Security Bulletin MS02-045:** "Unchecked Buffer in Network Share Provider May Lead to Denial-of-Service"
http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q326830&

UO network filtering policy. Due to a significant increase in attacks against campus machines via Windows File Sharing mechanisms, Network Services is now blocking SMB traffic from off-campus (see related article, "Network Services Blocks SMB Traffic…" on page 18).

Loopholes Surface

SQL Server 2000, Microsoft Exchange Server, Metadirectory Services 2.2

Last July, three new security holes were detected in Microsoft server and database products:

SQL Server 2000. The most serious of these flaws affects SQL Server 2000. It could allow an attacker to overwrite portions of system memory, perpetrating a denial of service attack or causing other system disruptions. For more information on this flaw, and to download the patch, see **MS02-039:** "Buffer Overruns in SQL Server 2000 Resolution Service Might Enable Code Execution"
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-039.asp

Microsoft Exchange Server 5.5. This flaw affects the server's Internet Mail Connector, which provides Simple Mail Transfer Protocol (SMTP). It could allow an attacker to trigger a buffer overflow, either crashing Exchange and blocking all inbound and outbound email delivery, or gaining complete control of the server. For more details, and to download the patch, go to **Microsoft Security Bulletin MS02-037:** "Server Response To SMTP Client EHLO Command Results In Buffer Overrun (Q326322)"
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-037.asp

Metadirectory Services 2.2. This flaw could enable a breach of privileged user access, allowing an attacker to bypass security checks and manipulate data that should, by design, only be accessible to administrators.

For more information on this flaw, and to download the patch, see **Microsoft Security Bulletin MS02-036:** "Authentication Flaw in Microsoft Metadirectory Services Could Allow Privilege Elevation (Q317138)"
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-036.asp

New Service Pack for Windows 2000 Contains a Bundle of Fixes

In August, Microsoft released Service Pack 3 for Windows 2000. The latest release is a hefty collection of bug and security fixes (including the fix for the SQL Server 2000 vulnerability outlined above), updates, and new middleware.

You can download the new Windows 2000 service pack from
http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/default.asp
or order it on CD (**http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/ordercd.asp**)

Probing Internet for Open Usenet News Servers Not Permitted

We've recently received complaints from sites on the Internet whose Usenet News servers were probed by a UO-connected desktop. This machine was apparently running NewsPro, a Usenet News software program that has the ability to try to connect to large numbers of news servers that are found by checking Usenet's "Path" field (see **http://www.usenetopia.com/pubsrv.htm**).

Use of this or similar tools that attempt unauthorized access to network resources (particularly tools that enable wholesale probes) is contrary to the university's Acceptable Use Policy as well as ORS 164.377(4), which states:

> **Any person who knowingly and without authorization uses, accesses or attempts to access any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime. [http://www.leg.state.or.us/ors/164.html]**

"Computer crime," as defined by that Oregon statute, is a Class A misdemeanor.

Use of network scanning/probing tools may also result in termination of your access to UOnet and/or disciplinary action by the university.

UO users who want to read Usenet News are welcome to use either of two locally provided Usenet News servers: **news.uoregon.edu** or **platform.uoregon.edu**

Questions?

If you have doubts about the advisability of running any program or program feature, please contact the Computing Center's Acceptable Use Officer, Jon Miyake (*miyake@darkwing.uoregon.edu*) before proceeding.

More Security Advisories in the News..

SecureCRT 2.x, 3.x, and 4.0 (SSH1 connections only)

This vulnerability, which could allow attackers to execute arbitrary code on the machine where SecureCRT resides, is specific to SSH1 connections. SSH2 server connections are considerably more secure, and users are urged to migrate to SSH2 as soon as possible. VanDyke Software, which designs SecureCRT, recommends that all users of versions 2.x and 3.x upgrade immediately.

Get the fix: To get a full description of the vulnerability and links to the appropriate fixes, go to **http://www.vandyke.com/products/securecrt/security07-25-02.html**

OpenSSL

Several potentially serious vulnerabilities were spotted in these versions of OpenSSL. (*Note that 0.9.td servers on 32-bit systems with SSL 2.0 disabled are not affected.*) The security holes leave systems open to remote attack and buffer overflow.

These flaws affect 0.9.6d or earlier, 0.9.7-beta 2 or earlier, and current development snapshots of 0.9.7 to provide SSL or TLS (whether client or server). It is probable that SSLeay is also vulnerable.

Details of this security advisory are available at **http://www.openssl.org/new/secadv_0020730.txt**

Remedies:

- Disable client altogether until patches are applied.
- Apply the patch to OpenSSL 0.9.6d (**http://www.openssl.org/news/patch_20020730_0_9_6d.txt**), or upgrade to OpenSSL 0.9.e. (*Note to UOnet users:* If you're on UOnet, you may download 0.9.e from **ftp://ftp/security/openssl/source/openssl-0.9.6e.tar.gz**)
- Recompile all applications that use OpenSSL to provide SSL or TLS.
- Get the combined patches for OpenSSL 0.9.7 beta 2 **http://www.openssl.org/news/secadv_20020730_0_9_7.txt**

PHP 4.2.0 and 4.2.1 (all platforms)

This vulnerability has the potential to allow attackers to compromise the web server and gain privileged access.

Remedy: Upgrade to PHP 4.2.2, which incorporates a fix for this flaw. You may download the updated version from **http://www.php.net/downloads.php**, or get it from one of PHP's mirror sites at **http://www.php.net/mirrors.php**

XDR libraries flaw affects Windows, Mac, Linux

Security watchdog CERT recently reported a flaw in SunRPC-derived XDR libraries, a widely used Sun Microsystems' communications technology. The flaw also affects the administration system of Kerberos 5, another commonly used authentication tool.

Although the library was originally distributed by Sun Microsystems, many other vendors have vulnerable code in their own implementations. Systems affected thus far include Mac OS X, Red Hat, Debian, FreeBSD, Sun, and NetBSD.

Possible exploits of this vulnerability include denial of service, execution of arbitrary code, or exposure of sensitive information.

For details, see CERT® Advisory CA-2002-25: "Integer Overflow In XDR Library" at **http://www.cert.org/advisories/CA-2002-25.html**

Remedies:

- Apply the patch from your vendor, or obtain updated XDR/RPC libraries (links to these are on the CERT advisory site at **http://www.cert.org/advisories/CA-2002-25.html**).

- Restart dynamically linked services that use XDR/RPC libraries.

- Recompile statically linked applications using the patched or updated XDR/RPC libraries.

- Disable all services that are **not explicitly required.**

Upgrade to avoid Flash Player security flaws

Last August, Macromedia warned that older versions of its Flash Player software, estimated to appear on 90 percent of all PCs, have a security flaw that could allow hackers to execute malicious code on Windows and UNIX-based operating systems. The flaw can be exploited in any program that employs an embedded Flash file, creating a buffer overflow in the Flash Player itself.

The latest versions of Flash Player are not vulnerable. You can download the latest versions for all platforms from Macromedia's download site at **http://www.macromedia.com/shockwave/download/alternates/**

For more details, see Matthew Broersma's article in *ZDnet*, " Flash flooded by security flaws" at **http://zdnet.com.com/2100-1104-949344.html**

Tips for Installing Latest Windows 2000 Updates

Having problems with the Add/Remove Programs Tool? Read on…

If you discover that Add/Remove programs no longer work after installing some Windows 2000 updates, you're not alone.

Microsoft has documented a bug associated with Internet Explorer 5.5 and 6 that interferes with the Start-> Control -> Add/Remove Programs function. For details, see Microsoft Knowledge Base Article Q265829 at

http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q265829&

To fix the problem, start by reinstalling IE. If you continue to have problems, run REGSVR32 APPWIZ.CPL from a CMD window, as described in Microsoft Knowledge Base article Q266668 at

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q266668

Mozilla, XEmacs Updates Installed on Darkwing

Over the summer, systems staff installed the latest versions of Netscape's Mozilla software and the XEmacs open-source text editor on Darkwing.

The new version of Mozilla (1.1a) is explicitly built for Solaris 2.7, Darkwing's current operating system. The XEmacs update (v. 21.4.8) included the new "SUMO Tarball" lisp library under **/usr/local/lib/xemacs**.

Faculty Instructional Technology Training Center Update

The Faculty Instructional Technology Training (FITT) Center has revved up its operations again this fall to meet the growing demand among UO faculty and GTFs for personal support in the use of instructional technology and multimedia. The FITT Center, located in Room 19 in Media Services on the ground floor of the Knight Library, offers free one-on-one instruction in web publishing, Blackboard support, presentation development, digital video, scanning, and other useful technology tools.

Regular drop-in hours are Monday through Friday from 11 A.M. to 6 P.M., or call ahead (**346-1942**) to schedule an appointment. For more information about FITT Center services, see

http://libweb.uoregon.edu/fittc/

BACKWARDS?

SEE: **http://www.alltooflat.com/geeky/elgoog/**

Mathematica 4.2 Ready to Install

Hans Kuhn
User Support Specialist
hak@oregon.uoregon.edu

Mathematica 4.2 is now available for installation. The password for version 4.1 works with the new software. Here are the download sites for Windows, Macintosh, and Unix versions:

Windows 98/NT/2000/XP: To download Mathematica 4.2 for Windows, go to **ftp://public.uoregon.edu/software/Mathematica/**

Macintosh: To download, go to CC Public Domain and open the following folders: Applications and Updates->Mathematica

Unix versions: You can check these out from the Computing Center Documents Room in 175 McKenzie.

Questions? If you have any questions about upgrading to the latest version of Mathematica, contact Hans Kuhn (**346-1714**, *hak@oregon.uoregon.edu*)

Got Melior?

By now, most, if not all, departments on campus should have received a copy of the Melior font CD from the Office of Publications.

Melior is now the official typeface for the university, and the CD, which was created by the Computing Center's Microcomputer Services group, makes installing the new font easy for both Windows and Macintosh users campuswide.

If your department has not yet received a copy of the Melior CD, please contact Barbara Oppliger in the Office of Publications, 346-5397.

COMPUTING CENTER GUIDE

UO Website
http://www.uoregon.edu/

Computing Center Website
http://cc.uoregon.edu/

Microcomputer Services
(151 McKenzie Hall)

- microcomputer technical support
- help with computing accounts, passwords
- scanning, CD-burning, digital video
- help with damaged disks, files
- system software help
- Internet connections, file transfers
- public domain software, virus protection
- software repair (carry-in only, $60/hour, 1/2 hour minimum)

346-4412
microhelp@lists.uoregon.edu
http://micro.uoregon.edu/

Documents Room Library
(175 McKenzie Hall)

346-4406
http://darkwing.uoregon.edu/~docsrm

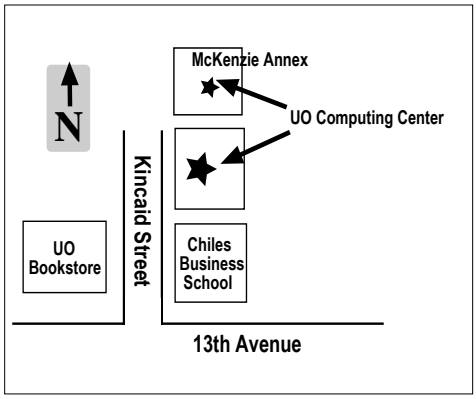
Modem Number
Dialin modem number for UOnet, the campus network: **225-2200**

Large Systems Consulting
(225-239 Computing Center)

- VMS, UNIX
  (Gladstone, Darkwing, Oregon)
- email, multimedia delivery
- scientific and cgi programming
- web page development
- statistics

346-1758
consult@darkwing.uoregon.edu
consult@gladstone.uoregon.edu
consult@oregon.uoregon.edu

http://cc.uoregon.edu/unixvmsconsulting.html



Electronics Shop (151 McKenzie Hall)
Computer hardware repair, installation, and upgrades.
346-3548
hardwarehelp@oregon.uoregon.edu
http://cc.uoregon.edu/e_shop.html

Network Services
Provides central data communication and networking services to the UO community.
346-4395
nethelp@oregon.uoregon.edu
http://ns.uoregon.edu/

Administrative Services
Provides programming support for administrative computing on campus, including BANNER, A/R, FIS, HRIS, and SIS. Call **346-1725**.

Computing Center Hours

Mon - Fri	7:30 A.M. - 5:00 P.M.

McKenzie Building Hours*

Mon - Thu	7:30 A.M. - 11:30 P.M.
Friday	7:30 A.M. - 7:30 P.M.
Saturday	9 A.M. - 9:30 P.M.
Sunday	9 A.M. - 8:30 P.M.

* Note: These are building access hours; hours for individual facilities may vary.

COMPUTING NEWS
UO COMPUTING CENTER
1212 UNIVERSITY OF OREGON
EUGENE, OR 97403-1212