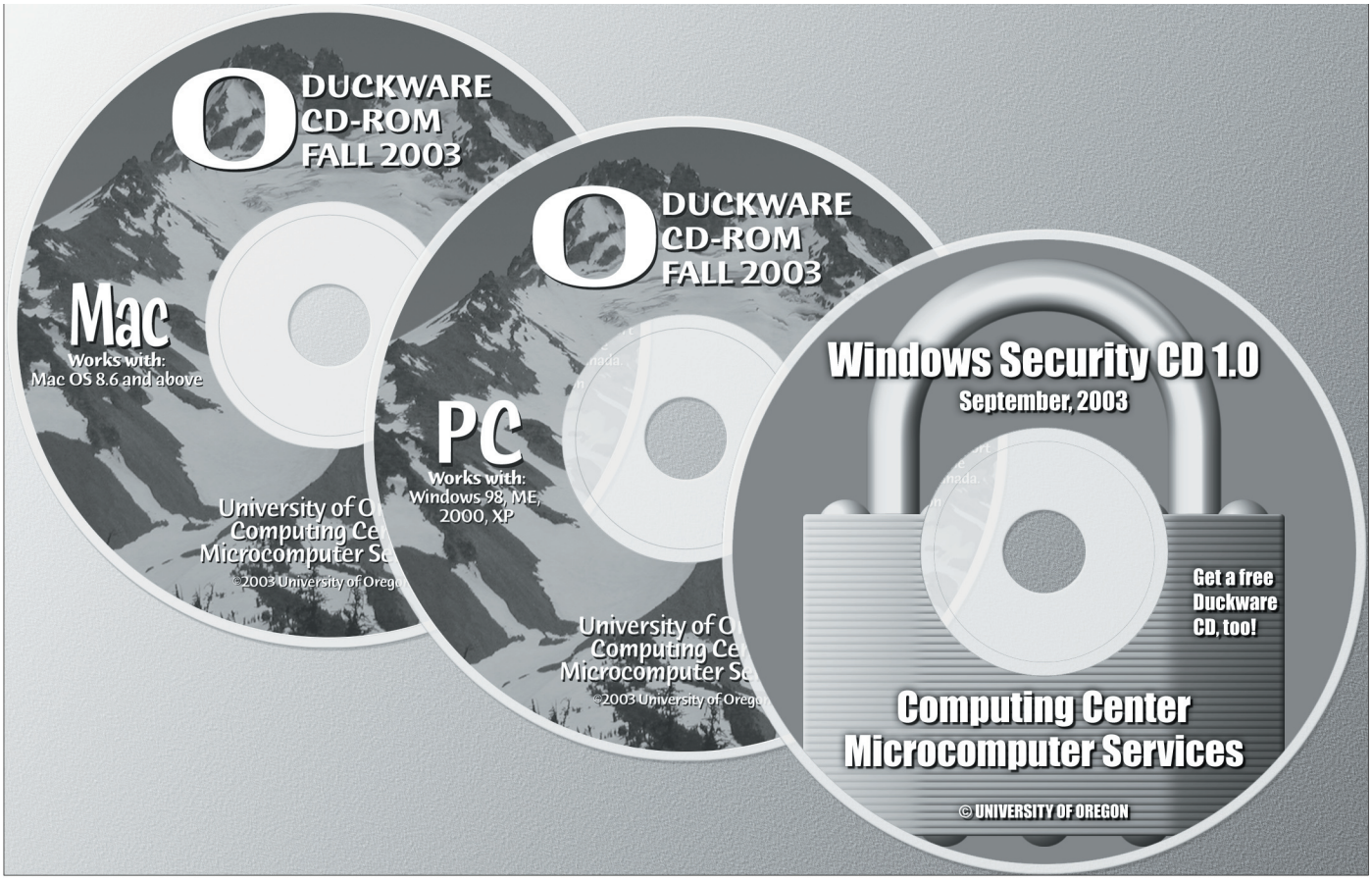
University of Oregon

COMPUTING NEWS

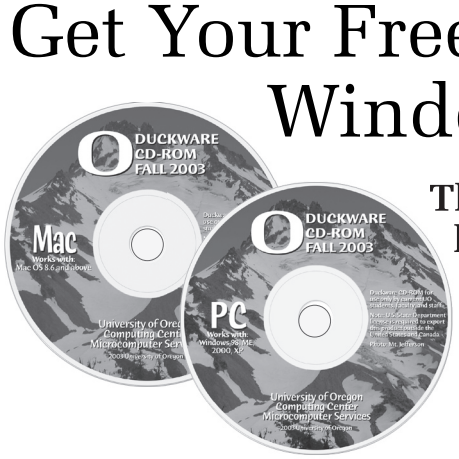
FALL 2003

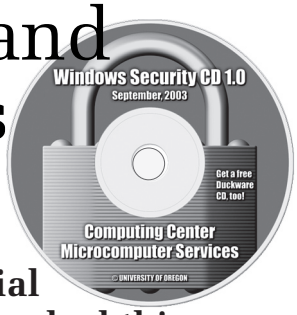


Get your free copy of Duckware 2003 for Mac or PC! The discs are distributed at numerous campus locations. New this year is a special supplementary Windows Security CD for Windows users. See stories on pp. 2, 17.

IN THIS ISSUE...

Get Your Free Duckware 2003—and Windows Security!—CDs





The latest edition of Duckware has just what you need for computing at the UO. For Windows users, a special supplemental security CD is part of the deal this year.

As it has every fall for the past seven years, the Computing Center's Microcomputer Services group has released a new edition of the Duckware CD-ROM.

Duckware 2003, a collection of the latest antiviral, network, and word-processing software designed to help you with computing at the UO, is available in both Mac and PC versions and is free to all currently enrolled students, faculty, and staff.

Both versions contain step-by-step instructions on how to use the university's modem pool, wireless network, and VPN connections.

Windows Users. This year's Windows edition includes Norton AntiVirus 2003, OpenOffice 1.1 for Windows, Internet Explorer 6, Netscape 7, Mozilla 1.4, and more.

New! Windows Security CD: UO Windows users will also need to pick up a copy of the new Windows Security CD, which contains vital antiviral updates and system patches specific to Windows machines. *Be sure to run this CD* ***before*** *you connect to the campus network!!*

Mac Users. The Mac Duckware CD contains Norton AntiVirus 9, Fugu 1.0, Mozilla, Internet Explorer, Netscape, and an updated and improved VPN client, among other offerings.

Because the Mac operating system is immune to the Blaster worm and other viruses that target Microsoft products, Mac users do not need a supplemental security CD.

System Requirements

PC users: To use Duckware 2003 for Windows, you'll need Windows 98, ME, 2000, or XP.

Mac users: The Macintosh version is compatible with Mac OS 9 and Mac OS X.

Where to Get Your CDs

Campus locations. Students, faculty, and staff may pick up a copy of the Duckware 2003 CD and Windows Security CD at the following campus locations:

- Microcomputer Support Center (151 McKenzie Hall)
- Documents Room Library (175 McKenzie Hall)
- CC-McKenzie Lab (101 McKenzie Hall)
- CC-EMU Microcomputing Lab (22 EMU)
- CC-Klamath Lab (B13 Klamath Hall)
- CC-Millrace Lab (113 Millrace I)
- Knight Library Information Technology Center (second floor)
- Science Library Information Technology Center (lower level, Onyx Bridge Building)

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 2003, 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."

Help

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

You can also drop by 151 McKenzie Hall weekdays from 9 A.M. to 5 P.M., or visit their website at **http://micro.uoregon.edu/**

UNIVERSITY OF OREGON

COMPUTING CENTER

COMPUTING NEWS

VOL. 18 #4

Computing News is published quarterly by the User Services and Network Applications staff of the Computing Center.

Contact: Joyce Winslow
jwins@oregon.uoregon.edu

Photography: Dave Ragsdale
dave@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

Got Extras?

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

Welcome to Campus!

How to Start 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 the handout, "How to Get a Computing Account," available in the Documents Room Library (175 McKenzie Hall), or online at **http://cc.uoregon.edu/policy/get_account.html**)

How Do I Start Using Email?

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 from your web browser (**https://password.uoregon.edu/authorize/**)

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 mixed-case letters and numbers. 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 Off-Campus Connections?

Your computing account username and password are the same ones you'll use for accessing UOnet from off-campus, whether you're dialing in with a traditional modem or connecting via the UO's VPN service through commercial DSL or cable modem service.

Traditional modem. If you're 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. You should also be aware that we have recently installed security filters that inhibit the use of Microsoft networking from dialup modems. If you really need to use Microsoft networking, the workaround is to install and run the VPN software included on Duckware.*

High-speed DSL or cable modem connections. If you have an account with a commercial Internet Service Provider, you may want to log in to your UO account using the UO's Virtual Private Network (VPN) software. VPN allows you to securely access resources normally restricted to on-campus use—such as the UO's software distribution sites, UO Usenet News servers, or restricted library databases. If you do *not* use VPN, for security purposes we recommend using end-to-end encryption tools (such as the SSL included in your web browser, or SSH for shell and file transfer).

For a good overview of VPN, see Microcomputer Services' general information page at **http://micro.uoregon.edu/getconnected/vpn_overview.html** Instructions for connecting to VPN are available at **http://micro.uoregon.edu/getconnected/**

What About Wireless?

You can also access UOnet throughout several public areas on campus via an 802.11a or 802.11b card in your laptop computer. Your device must have appropriate drivers for your wireless card and a web browser that supports SSL encryption. To connect to UOnet, you will need to authenticate with your Darkwing or Gladstone account username and password.

Security Note: Wireless users are especially vulnerable to electronic eavesdroppers. If you're using a wireless device and an application that lacks end-to-end encryption, you may wish to use the VPN software for added protection.

For more information on campus wireless and current areas of coverage, including detailed set-up instructions, see **http://micro.uoregon.edu/wireless/**

What About Campus Housing Connections?

Every room in every UO residence hall has an ethernet connection (ResNet). Your computer 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://housing.uoregon.edu/resnet/**

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, including how to get your new student computing account information. The Help Desk is also one place you can pick up your copy of Duckware and the Windows Security CD.

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
- how to get your new student computing account information
- password problems
- how to transfer files
- virus problems and protection
- system software configuration, troubleshooting, and installation
- damaged files and disks
- how to access public domain software

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 $80.00/hour, billed by the quarter hour. Typical problems requiring machine check-in 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. *New! As a convenience to customers, Microcomputer Services now accepts Visa and MasterCard.*

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

Hardware and software in all the computing labs managed by the Computing Center have been upgraded for fall term. Many of the labs are equipped with new 2.6 GHz Dell Pentium 4s running Windows XP Pro and 1 GHz iMacs running Mac OS X.

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. New software this year includes Macromedia Director MX, Maya 5, InDesign, and Premiere 6.5.

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 (*labhelp@darkwing.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. 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 has been outfitted with all-new Dell Pentium 4s for fall.

Computing Center's E-Shop is Set to Handle All Your Microcomputer Repairs and Upgrades

Conveniently located on campus in 151 McKenzie Hall, the Computing Center's Electronics Shop's experienced technicians offer extensive personal computer hardware support and repair services to UO students, faculty, and staff.

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. The shop also offers non-warranty repairs 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 or Intel-based desktop computers, and other items can be ordered upon request.

Custom Systems (including backup solutions such as Firewire/USB and CD-RW drives or DVD superdrives). 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.

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

E-Shop technician Robert Bennett repairs a laptop. The shop also stocks a wide selection of parts and popular backup solutions such as the thumb drive (see below).

Rates. Upgrades and out-of-warranty repairs are charged on a time-and-materials basis. The initial diagnostics fee is $40, and the current labor rate is $80/hour, billed by the quarter hour.

New! As a convenience to customers, the shop now accepts Visa and MasterCard.

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.

Weekends. 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 **346-3548**.

Compact USB Thumb Drives Offer Nifty Storage Solution

Lightweight USB Flash Drives are a handy backup-and-go solution. These colorful translucent drives, barely bigger than your thumb, are small enough to fit on your key chain and can be plugged into any USB port. No power supply or cables are needed.

Despite their toylike appearance, the drives have a lifetime of up to one million rewrites and can retain data for up to 10 years.

The E-Shop stocks USB thumb drives in four sizes: 16MB ($15), 64MB ($30), 128MB ($50), and 256MB ($75). A fifth size, 512 MB, will also be available soon.

Detailed product information is also available at the vendor's website:

http://usbkeydrive.com/USB_Drive.htm

Technical Information and Training Resources: the Computing Center Documents Room

Build your tech skills with Docs Room's "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 Library (175 McKenzie) has a growing collection of training materials covering such popular applications as Photoshop, Dreamweaver, PageMaker, Flash, InDesign, and the various Microsoft Office products, as well as the Mac OS and Windows operating systems.

These tapes and CD-ROMs are movie-based tutorials that include several hours of instruction by experts skilled in software training. The CDs feature high-quality visuals, especially noticeable in the shots of computer screens.

Two of our most recent acquisitions are *Learning Illustrator 10* and *Learning GoLive 6,* both from the publisher lynda.com (Lynda Weinman).

To see a complete list of the training CD-ROMs and videos, go to **http://docsrm.uoregon.edu/** and type "training." Then hit "search."

Books and magazines. In addition to its collection of videos and CD-ROMs, the Documents Room offers books and magazines on a wide range of computing topics including computer security, Linux, Java, handheld computers, and web design and creation. You can search its catalog 24 hours a day at **http://docsrm.uoregon.edu/**

Books circulate for two weeks, videos and CD-ROMs for one week, and magazines for two days. All materials are renewable, unless another patron has requested the item.

Contact Information. The Documents Room is open 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 —

Find out what system resources are available to you

Faculty/Staff

Faculty and staff will normally use Darkwing, a large shared Sun Enterprise 5500 Unix system targeted for compute-intensive academic applications as well as email and web access.

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 (forwarding instructions are available at **http://cc.uoregon.edu/mailforward.html**).

Undergraduate Students

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

Among other things, 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 create 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. For more details on administrative systems, see the Administrative Services website at **http://ccadmin.uoregon.edu/**

Off-Campus Access

Your account on Darkwing or Gladstone enables you to dial in from off campus to the university's modem pool (see "What About Off-Campus Connections?" on page 3.) 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 will want to contact a commercial Internet Service Provider. One list of ISPs is available at **http://www.thelist.com/)**

DSL and cable modem subscribers can connect via the UO's Virtual Private Network, or VPN (you'll find an overview of VPN online at **http://micro.uoregon.edu/getconnected/vpn_overview.html**). Software to access the Internet and campus facilities from home is available on the Duckware CD-ROM, which is free to all faculty, staff, and registered students (see article on page 2). You may also acquire shareware from the Computing Center's public domain libraries (**http://micro.uoregon.edu/pd/**).

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 Help

If you have any questions about using the UO's large timesharing computers, contact the large systems consulting group in 225-239 Computing Center (**346-1758**, *consult@darkwing* or *consult@gladstone*). 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 2003 CD (see article on page 2). See also **http://www.symantec.com/avcenter/**
- **SAS.** SAS users may 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://esri.uoregon.edu/**

Statistics Consulting

If you need help with a statistical analysis project, make an appointment with Robin High, the Computing Center's resident statistical consultant. Call **346-1718** or write *robinh@uoregon.edu* to make arrangements.

You may also want to visit Robin's statistical resources page at **http://darkwing.uoregon.edu/~robinh/statistics.html**

This page offers guides for using SAS, SPSS, and MINITAB, as well as essays on pertinent data analysis issues.

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) spam assassin	ftp (remote file transfer) lynx (web browser) pine (email) trn, tin, nn (USENET News) ssh (secure login) pgp (encryption) spam assassin
X Window Only	netscape (web browser) xv (image manipulation) openoffice (Office Suite) acroread (Acrobat Reader) gimp	netscape (web browser) xv (image manipulation) openoffice (Office Suite) acroread (Acrobat Reader) gimp
Programming	cc and gcc c+ and g++ f77, f90, f95 (FORTRAN) pc (Pascal) NCAR fortran graphic libs Java developer's kit tcl/tk	cc and gcc c+ and g++ f77, f90, f95 (FORTRAN) pc (Pascal) 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, as well as links to frequently asked questions about using email at the UO and other helpful resources, see the Computing Center's "Email at the UO" section at **http://cc.uoregon.edu/email.html**

Administrative Computing Update: Web-Based Banner is Here!

Campus Banner and Data Warehouse users will notice some changes this fall…

Susan Hilton
Director, Administrative Services
hilton@oregon.uoregon.edu

This summer has been a busy one for the developers who support Banner.

We've upgraded to Oracle 9i, installed a number of interim Banner "point" releases, and added considerable functionality to the data warehouse. We've also continued to enhance system security and are working to reduce unscheduled downtime by providing additional redundancy of our systems.

The big news is that the web-based version of Banner, Internet Native Banner (INB), is now available at the UO. People have quietly begun using it and initial reports are very favorable. We continue to address some of the issues that accompany any conversion and should have most of them resolved very shortly.

With INB, Banner users will no longer need to log on to the Banner Windows NT domain or map a drive to Huey or Dewey in order to run Banner. For more details on using the new version of Banner, including answers to frequently-asked questions, please see **https://inb.uoregon.edu/**

Complete your migration to INB before Thanksgiving. When Banner 6.0 is installed on Thanksgiving weekend this year, the current client-server method of running Banner will no longer be supported. This means everyone will need to be using INB before that date.

Data Warehouse. Data Warehouse users will also be impacted by the demise of the old client-server mode. They will need to install the Oracle networking software, Sql*Net, on their desktops rather than accessing it from the file servers Huey and Dewey.

We've developed an installation program that will remove Huey/Dewey from the user's Windows PATH environment variable and install Sql*Net. The program is available for download at **http://ccadmin.uoregon.edu/banner/dwhs_install.shtml**

Long-term plans include working with Oregon Hall and representatives from departments to look at other Data Warehouse solutions, perhaps one that is web-based.

What about LDAP? An unrelated topic that people are asking about is the LDAP (light directory access protocol) directory.

After a long delay in equipment delivery, we finally received the hardware and have begun work configuring the directory service. Our first project will be to rewrite the online directory to utilize the new LDAP- based directory service. We will provide more detailed information as we progress.

Questions?

To learn more about administrative computing services and staff, see **http://ccadmin.uoregon.edu/**

Prepare to Move from Oregon to Darkwing

As most of you know, by fall 2004 we will have discontinued service on Oregon, the academic OpenVMS system (administrative users on Daisy and Donald are not affected).

Now would be a good time to move your email and web pages off Oregon and onto Darkwing or Gladstone. (Note that new Darkwing addresses may be shortened to the form *username@uoregon.edu*)

Beat the rush. It would be a good idea to migrate sooner rather than later. That way, you'll have it in time to meet publication deadlines for directory updates, as well as reprints of business cards and other official stationery. Currently enrolled students, faculty, and staff will find instructions* for migrating their mail from Oregon to Darkwing or Gladstone at **http://cc.uoregon.edu/cnews/fall2002/mailmove.html**

Information resources. For details on the Oregon system phase-out, see the Fall 2002 *Computing News* article at **http://cc.uoregon.edu/cnews/fall2002/oregonout.html**

Special heads-up for list owners: The Computing Center's Listmaster has put together some vital online tips for list owners to help them update their list subscriptions in time for the migration:

- "The Great Change" (**http://darkwing.uoregon.edu/~majordom/great-change.html**) A useful set of tools to help you manage various facets of the migration.
- "Moving Day" (**http://darkwing.uoregon.edu/~majordom/moving-day.html**) Five easy steps for moving your email to Darkwing and updating your list subscriptions.

*** Note to UO Faculty Emeriti:** Instead of following these instructions, please contact Lucy Lynch (*postmaster@lists.uoregon.edu*, **346-1774**) for help with the migration.

UO Prepares for Increasing Wireless Use on Campus

With the growth of wireless networks, there's no need to stay tethered to a network jack

Greg Bothun
Professor, Department of Physics
nuts@bigmoo.uoregon.edu

Students work on an assignment in the wireless classroom in 204 Condon.

Networking is rapidly moving towards wireless communication. Indeed, all of technological society is moving to an "on-demand" and location-independent mode of information access, with high throughput.

In principle, if you have the proper wireless network appliance, you should be able to be anywhere on the planet that has wireless connectivity and access your favorite site on the Internet.

Here at the UO, we recognized early on that wireless would become an increasingly important component of our basic network infrastructure. Since the year 2000, Network Services, largely funded by student Ed Tech dollars, has worked aggressively to build out wireless access throughout the campus community, including many outdoor spaces.

These days, increasing numbers of students can be observed accessing the wireless network from various locations on campus. Indeed there are even whole classrooms in which the use of wireless laptops by students is an integral part of the course. Those particular classrooms (Condon 204 and Library 41/42) provide students with wireless laptops, but students can use their own wireless laptops there as well.

Students purchasing new laptops should most definitely be searching for those that have "integrated wireless" capability. In geek-speak, that means the laptop is 802.11b, 802.11a, and/or 802.11g compliant.

At the UO, our main wireless standard is 802.11b, but in early 2004 we will be installing 802.11g equipment; the data rate for g is about five times that of b.

Students contemplating wireless options should be aware that many versions of the Palm Pilot or the Pocket PC are now wireless compliant. This means you won't necessarily need a laptop to access UO wireless and the global Internet.

Although the display on these hand-held devices is generally limited to 320x240 pixels, it still allows you to access some useful information.

For example, the UO has recently invested in a new video-on-demand (VOD) technology that, among other things, can offer students indexed video replays of class lectures. So it's possible that some day in the future, if you wanted to review the two minutes of the lecture in which the prof said "this is going to be on the midterm," you could conceivably have the streaming video and audio delivered to you most anywhere on campus via your PDA.

Wireless access to the campus network and the global Internet has many potential benefits to the campus community. Information can now flow more easily from place to place and you can access it without being tethered to a network jack. Indeed, in the wireless world, students would always be "jacked in."

Network Services will continue to increase the coverage and efficiency of wireless networking on the UO campus. In turn, students should start to pay attention to this new service and the kinds of wireless network appliances that are available.

Resources

More information on campus wireless, including set-up instructions, is available on the Microcomputer Services information page at
http://micro.uoregon.edu/wireless/

For a discussion of home network configurations, including wireless components and standards, you may want to visit Microcomputer Services "Home Networking" page at
http://micro.uoregon.edu/homenetworking/

UO Libraries' Tech Services Continue to Grow

Ron Renchler
Director, Library Communications
ronr@darkwing.uoregon.edu

This fall, the University of Oregon Libraries will greet returnees and new users with several new or upgraded services, as well as its usual menu of technology-related training programs—all designed to help students and faculty in their academic studies and research:

Laptop Loan Program

Nine laptops—seven Dell Latitude D600 (Windows) and two Macintosh iBooks—are available to students for checkout in four-hour blocks on weekdays and for longer periods overnight and on weekends.

The machines are preloaded with popular software and have network connectivity and printing capabilities. The UO Libraries' Media Services Department, located in Knight Library, is handling the checkout process. For complete information about the laptop loan program, visit

http://libweb.uoregon.edu/med_svc/laptops/

Enlarged Union Catalog

Library patrons now have access to a greatly enlarged union catalog due to the merger of two library consortia, Orbis and Cascade, into the Orbis Cascade Alliance. The Alliance combines catalog records from the twenty-seven member libraries into one database, called Summit. UO faculty, students, and staff will be able to use Summit to borrow library materials from any Orbis Cascade Alliance member library. For more information, visit the "Orbis Cascade catalog" link on the UO Libraries' home page at **http://libweb.uoregon.edu/** or go to **http://summit.orbiscascade.org/**

IT Training Workshops

Software and technology training workshops for the entire campus community are offered through the libraries' Information Technology (IT) curriculum. See the complete schedule for fall at

http://libweb.uoregon.edu/it/

FITT Center

The Faculty Instructional Technology Training (FITT) Center provides personal consulting support for faculty and GTFs in the use of instructional technology and multimedia. Visit the FITT website at **http://libweb.uoregon.edu/fittc/**

24/7 Program

Students were ecstatic last spring during Dead Week and Finals Week when the doors of Knight Library remained open twenty-four hours a day. Campus patrons will be happy to know that the 24/7 program will again be in place during those critical two weeks at the end of each academic term in 2003-4. A current university ID will be required for library use during all extended hours, and services will be limited to study space, photocopy machines, and Information Technology Center (ITC) computers and printers.

Blackboard 6

A new and improved version of Blackboard, the UO's course management and delivery system managed by the UO Libraries, is set for launch this fall. See the article below for more information.

Blackboard Upgrade Introduced This Fall

Over the past several months, the Computing Center and the University of Oregon Libraries have collaborated to launch Blackboard 6, the latest version of the online course administration and delivery system used at the UO.

Version 6 provides instructors with more flexibility in content management and sharing, better assessment and assignment management, and a new Virtual Classroom tool that facilitates collaboration and communication in the learning environment.

Students log in to Blackboard 6 using their Gladstone or Darkwing email address and corresponding password (e.g., *jdoe@gladstone* and the appropriate password). Faculty and GTFs using version 6 will see some procedural changes when developing their courses. Blackboard 6 support for both faculty and students is available at **http://blackboard.uoregon.edu/**

Individuals with questions about the upgrade or departments interested in scheduling training workshops for their teaching staff should contact JQ Johnson, the UO Libraries' academic education coordinator (**346-1746**, *jqj@darkwing.uoregon.edu*).

The Blackboard system is managed by the UO Libraries with collaborative support from the UO Computing Center.

Simple Passwords Expose Your PC to Attack by 'Backdoor' Worm

Protect your machine from a malicious takeover: choose a secure password!

Jon Miyake
Acceptable Use Policy Officer
miyake@uoregon.edu

On July 2, several Windows machines on campus were infected with the Backdoor.IRC.Flood.E worm before security personnel were able to shut it down. The virus, an IRC Trojan that scans for Windows machines and attempts to log in to them with a defined set of simplistic passwords, contaminated all of these campus machines in less than 30 minutes.

Backdoor.IRC.Flood.E is nothing special: it's "just" your normal, nasty, self-propagating worm that allows remote users access to your computer and all of the data contained therein, and you can protect yourself by taking a few simple precautions—starting with taking care in selecting your Windows password.

How to Protect Yourself

Change your password. If your Windows login password can be found in a dictionary (foreign language or otherwise) or if it's a non-random series of letters (such as abcdef, qwerty, etc.) and/or numbers (e.g., 123456, 111111) then it is weak and can be easily compromised. If your Windows login password fits this description, please change it to something that is secure.

Run Norton AntiVirus and enable its AutoProtect feature. If you're not running NAV, please do so and be sure to activate "AutoProtect." The program is site-licensed to the University of Oregon for use by faculty, staff, and students, and is included on the Duckware 2003 CD (see Duckware article on page 2). You may also download it from **http://public.uoregon.edu**

Basic security checklist: Using a secure password, keeping your computer up-to-date with Microsoft's critical patches, updating your virus definitions, enabling NAV's AutoProtect, and scheduling regular full system anti-viral scans of your computer goes a long way toward protecting your PC.

This may seem like a long "to-do" list for the average user, but most of these tasks can be automated after they're initially configured.

More advanced precautions. If you're running a version of Windows that allows you to modify system policies, such as Windows 2000, you may wish to tighten remote access to your system and limit the information that it could provide to remote attackers. If you're running a server class version of the Windows OS (e.g., Windows NT, Windows 2000) go through and disable any services or daemons that you don't need or use.

Information Resources

For complete details on Backdoor.IRC.Flood.E, read Symantec's information page at
http://securityresponse.symantec.com/avcenter/venc/data/backdoor.irc.flood.e.html

If you have further questions or concerns regarding the Backdoor worm, please contact *security@uoregon.edu*

Update to Avoid Axis Network Camera Vulnerabilities

Users are urged to update vulnerable cameras ASAP

Core Security Technologies recently reported an authentication bypass for Axis Network Cameras that affects the following models:

- **AXIS 2100 Network Camera** 2.32 and earlier
- **AXIS 2110 Network Camera** 2.32 and earlier
- **AXIS 2120 Network Camera** 2.32 and earlier
- **AXIS 2130 PTZ Network Camera** 2.32 and earlier
- **AXIS 2400 Video Server** 2.32 and earlier
- **AXIS 2401 Video Server** 2.32 and earlier
- **AXIS 2420 Network Camera** 2.32 and earlier
- **AXIS 2460 Network DVR** 3.00 and earlier
- **AXIS 250S Video Server** 3.02 and earlier

The exploit is simple and requires only a web browser to make unauthorized changes to the camera's configuration. Left unchecked, the flaw could allow a malicious user to reconfigure the camera to use excessive bandwidth, change the ftp or email destinations for images, or even entirely disable the camera.

The good news is that a fix is readily available and is easily applied by updating the camera's firmware to the current release available at Axis's Support Website at
http://www.axis.com/techsup/firmware.asp?value=camserver

For more information on this exploit, see Core's advisory at **http://www.coresecurity.com/common/showdoc.php?idx=329&idxseccion=10**

Beyond the Basics of Windows Security:

Blaster, SoBig, and Slammer have upped the ante on securing Windows systems

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

With recent pernicious exploits such as "W32/Blaster," "W32/SoBig," and "SQL/Slammer" rapidly infecting large numbers of systems on the Internet, everyone from system administrators to the average PC user has become increasingly aware of the need for basic security.

Because of the increased frequency and severity of the attacks on Microsoft Windows computers, users have become much more savvy about protecting their machines. Antiviral software is now a basic requirement for the operation of a Microsoft Windows computer. Users are also becoming more aware of the importance of keeping their OS patches up-to-date by using the Windows Update site. System integrity, however, is one area of computer protection that is not being addressed by most users.

The Importance of System Integrity

The basic idea behind system integrity is this: by periodically monitoring the changes that occur to a computer's files and directories, it becomes a simple matter to later determine 1) if a machine has been exploited, and 2) what changes were made to the system by the exploit. Without system integrity, it is difficult to detect if an exploit has occurred, and next to impossible to perform a comprehensive cleanup of the machine, short of a complete OS and application reinstall.

Establishing a baseline. The mechanisms used to generate system integrity information are usually either simple file and directory attribute lists, or more complex cryptographic signatures that are generated by running the file through a computational filter which produces a unique key that can be used to identify the file. These attributes or signatures are stored in a database that can then be used to form a "baseline," or representation of a known, "good" state of the machine.

Successive runs of the system integrity software are compared against the baseline to look for changes. If the changes are warranted, such as when a new product is purchased and installed, the user can simply update the baseline. On the other hand, if the changes are unwarranted, they can show clear evidence that a machine has been infected. You will also be able to identify which files or directories have been added to the machine, or modified.

Tools for Maintaining System Integrity

Fortunately, the availability of useful system integrity tools is improving. In the past, these tools were not much in demand because they were expensive, hogged resources, and were often difficult to use. But that situation is beginning to change. Not only has Microsoft taken steps to generate system integrity information through various built-in mechanisms, but commercial products designed specifically for maintaining system integrity are proliferating. In addition, some current personal software firewall packages now include integrated system integrity components. These tools are discussed in more detail below.

Microsoft's Built-in Features

System Restore. The "System Restore" feature of Windows XP and Windows ME is a useful resource for maintaining system integrity. Users typically call on this feature when an application installation has caused problems and they wish to roll the system back to a previous state. System Restore checkpoints are created automatically by Windows during application installations, or periodically during system idle time. The checkpoints contain snapshots of system files, the system registry, and some application files.

"System Restore" operations and settings can be accessed through the "Start/Help and Support" menu, or directly through the "Start/Accessories/System Tools/System Restore" menu. While "System Restore" can be extremely helpful in certain circumstances, it is not a comprehensive integrity tool. Users are still encouraged to utilize "Add or Remove Programs" or the "Uninstall" shortcuts for removing unwanted software.

Windows File Protection. Windows ME, 2000, and XP also have a feature called "Windows File Protection." The most critical Windows system files, a core collection of **.sys**, **.dll**, and **.exe** files, are monitored by the system. If an incorrect version of a system file is installed, Windows automatically replaces the file with either the previous version or the original version from the installation CD. For more information on the details of this system, visit the Microsoft website and look for references to the SFC.EXE or "System File Protection" command.

WHQL Driver Signing. Windows ME, 2000, and XP also have a feature known as "WHQL (Windows Hardware Quality Labs) Driver Signing," which is a method of generating signatures for Windows device drivers. Hardware vendors submit their driver packages to Microsoft, whereupon Microsoft generates signature files to be added to their driver distributions. When a new driver is first installed or activated, Windows automatically checks the files against the signatures and users can then choose whether or not they wish to allow the driver to be added to their system.

A Guide to Protecting System Integrity

Higher-End Products

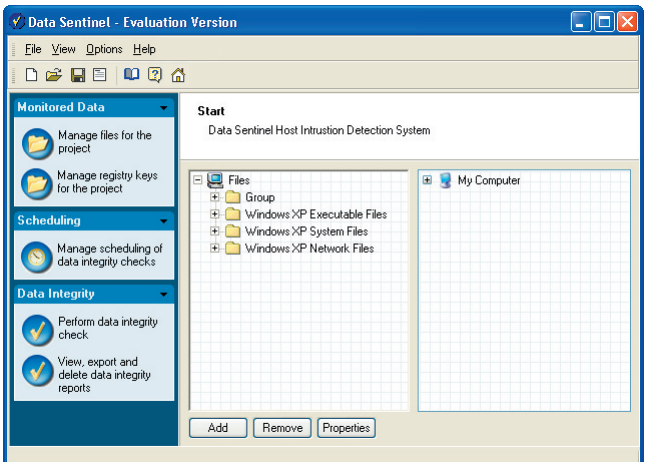
Some of the commercial Windows system integrity packages are listed below. Their feature sets vary tremendously. Packages are available for either single servers, or for multiple clients and servers which are distributed through a central management station. Some operate in near real-time, becoming active components of the system. Others run periodically and send out notifications through email. Some of the packages can also be integrated with network management consoles utilizing SNMP mechanisms. Four of these commercial packages are reviewed briefly below:

***1. Tripwire for Servers* (http://www.tripwire.com/):** The grand-daddy of these packages is *Tripwire*. *Tripwire* began as a free, command-line utility on Unix systems, but has since developed into a fully distributed, full-featured product for Windows. *Tripwire for Servers* 4.0 is the current standalone product. Perhaps the biggest complaint about *Tripwire* is that it is not an inexpensive product. Nevertheless, it continues to lead the field in this product category.

***2. Intact* (http://www.pedestalsoftware.com/):** The design of Pedestal Software's *Intact* program is an interesting variation in this product category. The two most prominent features of the package are anomaly detection and real-time monitoring. During the first few days after the product is installed, it monitors the system for normal activity. Later, it watches for changes that vary outside the norm of the observed behavior. This has the potential to reduce the number of false positives that other system integrity systems might generate. The real-time monitoring feature of *Intact* comes about through tight integration of the application with the primitive file actions of the operating system. Real-time notification can be an advantage for the administration of critical machines.

***3. Veracity* (http://www.rocksoft.com/veracity/)**: Rocksoft's *Veracity* product is available for number of different platforms. *Veracity* is reminiscent of the original *Tripwire*, in that it is invoked as a command-line application or run from a batch file. It will appeal to users who prefer command-line tools over GUI interfaces. *Veracity* has a flexible monitoring language that can be used to define what types of files and attributes to monitor. Perhaps the most notable feature of this application is the price, which is considerably lower than *Tripwire*, *Intact*, or *Data Sentinel*.

***4. Data Sentinel* (http://www.ionx.co.uk/):** *Data Sentinel* by Ionx is a more recent product that comes out of the UK. Its interface is probably the cleanest and easiest to use of any of the commercial products listed above. Coarse controls for doing either "fast" or "normal" checks on files are allowed. These kinds of features can produce checks that run much more quickly. Even the more rigorous file checks can run sufficiently fast, since *Data Sentinel* uses one of the more efficient cryptographic signature generation methodologies. Overall, *Data Sentinel* has a very clean, easy to use, and polished interface. Perhaps fittingly, the price of the product is somewhat high.



Data Sentinel's main program window.

Lower-End Products

For a good computer programmer, the process of producing a list of the files on a system and then generating a list of signatures for those files should be fairly simple. A number of respectable freeware, shareware or otherwise inexpensive programs are currently available for performing this task:

- *MD5summer* **http://www.md5summer.org/**
- Winalysis **http://www.winalysis.com/**
- *GFI LANguard System Integrity Monitor* (Freeware Version) **http://www.gfisoftware.com/**

MD5summer. *MD5summer* is "postcardware," that is, the author requests only that you send him a postcard if you find the product useful. As the name suggests, the program is used to generate MD5 cryptographic checksums of Windows files. While not as fast or clean looking as some of the high-end packages, the program has a fairly intuitive GUI interface, and checksums are saved to a simple file at the end of a run. Later, the file can be used by the application to verify that the current system checksums match those in the saved file. It becomes a relatively simple task to take a snapshot of the C:\WINDOWS directory and then check it again later for changes. *MD5summer* is designed to run on all Windows versions and is also available in a command-line version.

Winalysis. The *Winalysis* program is an inexpensive, lightweight system integrity checker. The GUI interface, while not quite as clean as some of the other programs in this roundup, is still fairly easy to navigate. Over time, the author has added additional features (such as file archiving) and improvements to the user interface to make it a more attractive product.

GFI LANguard. GFI Software is the maker of *GFI LANguard System Integrity Monitor*. GFI is perhaps better

Protecting Windows System Integrity, continued…

known for its commercial Network Security Scanner product, so it's a pleasant surprise to see GFI offer a system integrity product that's available as freeware.

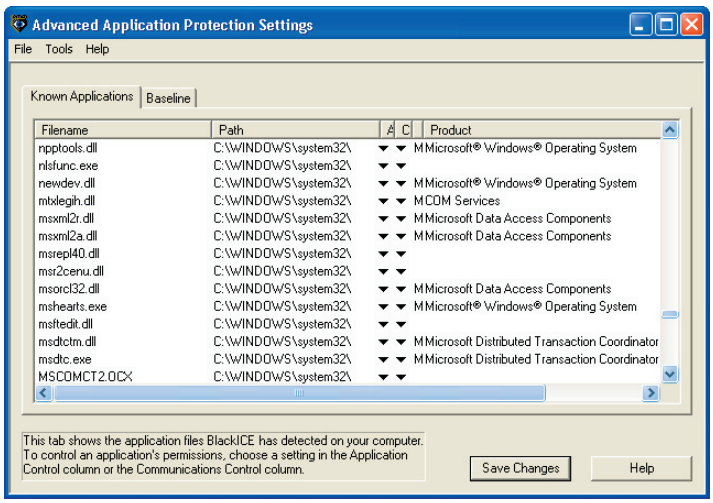
Any of the products mentioned in this section should be suitable for rudimentary system integrity checking.

Personal Software Firewalls

Personal Software Firewalls are fairly inexpensive, and their features and capabilities have developed over time. Some of the more popular packages are listed below. Along with the traditional features like address range, port number, and protocol filtering, these products often include additional protections such as ad blocking, cookie management, and Active-X and Java script controls. Some of these products also incorporate system integrity components:

- *BlackICE PC Protection 3.6*
  http://blackice.iss.net/product_pc_protection.php
- *ZoneAlarm Pro 4*
  http://www.zonelabs.com/
- *Sygate Personal Firewall PRO 5.1*
  http://smb.sygate.com/products/spf_pro.htm
- *Norton Personal Firewall 2003*
  http://www.symantec.com/sabu/nis/npf/
- *Tiny Firewall 5.0*
  http://www.tinysoftware.com/

ISS BlackICE PC Protection 3.6. *BlackICE PC Protection*, for example, has a feature called "BlackICE Application Protection." This component of the program looks for all system executable files, specifically those files which end with an extension such as: **.com .dll .drv .exe .ocx .scr .sys .vxd**. *BlackICE* builds a baseline database of these files that includes the associated file and directory size and modification times. Applications that do not appear in the database are considered "unknown." When an unknown or modified application is launched, it can trigger a popup prompt to appear, or the application can be automatically terminated. *BlackICE* includes similar features for controlling network access by unknown applications.

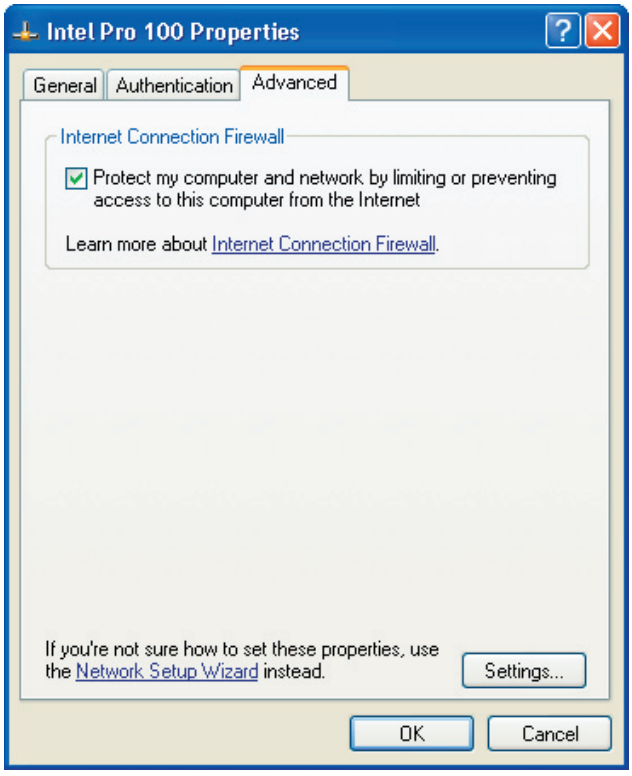


BlackICE Application Protection window.

Other programs in this category also include similar basic system integrity features. Both *Zone Alarm Pro 4.0* and *Sygate Personal Firewall 5.1* include basic system integrity monitoring mechanisms for applications that access the network. A checksum library is developed as network applications are used, and the applications are monitored for changes. In addition, **.dll** libraries are also monitored by these programs. Such features are becoming more common as a selling point because of the additional protection they can provide.

Conclusion: 'An Ounce of Prevention is Worth a Pound of Cure'

It is better to prevent a break-in from happening than it is to have to cleanup after a break-in has occurred. Most security professionals emphasize "intrusion prevention" over "intrusion detection," which is why the mantra of computer support personnel is "run antiviral software, keep your system patches up to date, and enable the Internet Connection built-in firewall if you're not running a server."



XP built-in Internet Connection Firewall.

Nevertheless, at some point most users wish they had a good snapshot of their system. That point usually comes immediately after they have discovered that their system has been infected. System integrity checking is only one piece in the puzzle of computer security, but clearly it's a valuable one—and one that is becoming more important every day.

The Terrible Trio: Three Common Types of Rogue Programs and How They Work

Trojan Horse

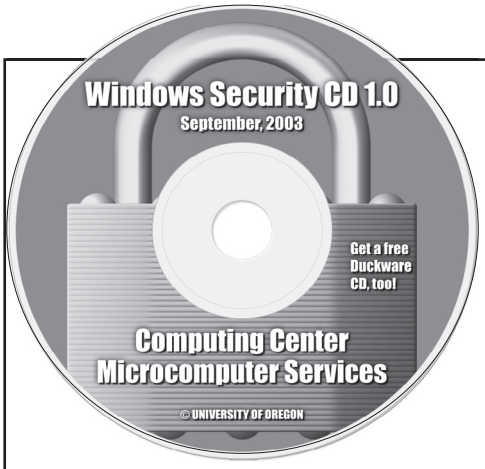
Like the treacherous steed of Greek legend, a trojan program comes disguised as a gift but packs an unpleasant surprise. Trojans frequently appear to be innocuous, such as applications found on the Internet or attachments to email messages. Trojans neither replicate nor copy themselves, but they cause damage or compromise the security of a computer.

Virus

A self-replicating program or code that can infect another program or maliciously modify its environment so that merely invoking an ordinary program could call up a possibly evolved copy of the virus. Most viruses only replicate, although many do a large amount of damage as well.

Worm

A self-contained program or set of programs that makes copies of itself, either from one disk drive to another, or by copying itself via email or another transport mechanism. "Host worms" are entirely contained in the computer they run on and use network connections only to copy themselves to other computers. "Network worms" consist of multiple parts, each running on different machines (and possibly performing different functions).



What You Need to Know about the New Windows Security CD

If you run Windows, use this Windows Security CD *before* connecting to the campus network!

Tell your UO friends and colleagues who run Windows to patch their systems immediately upon returning to the UO campus this fall.

The easiest way to patch your Windows system is to grab a free Windows Security update CD from Microcomputer Services in 151 McKenzie Hall or from the usual Duckware distribution points (see the Duckware article on page 2 for a complete list of these distribution sites). Like Duckware, the Windows Security CD is for UO faculty, staff, and currently enrolled students only.

Run the CD *before* connecting to UOnet. The infection rate of the current RPC worms (W32/Blaster, W32/SoBig, etc.) is so fast, users *will not* have time to download the updates from Microsoft's Windows Update site before becoming contaminated. *For this reason, you must use the security CD* ***prior*** *to connecting to the campus network.*

Ethernet users: don't connect to UOnet until you run the CD. Returning students and staff should *physically unplug their ethernet cable*, run the security CD, then plug the ethernet cable back in when the CD's protective cycle is complete.

Dialin users: Dialin users should run the security CD *prior* to dialing in.

How the CD Works. Like Duckware, the Windows Security CD automatically plays when inserted into your computer's CD-ROM drive. The program on the Security CD checks to see if your system is already infected, and if it is, tries to remove any exploits. It applies the appropriate patch for Windows 2000 or XP systems (Windows ME, 98, and 95, and all Mac OS systems are not affected). As a final measure, virus definitions are updated and a scan is invoked.

Keep a record of any error messages. Users need to pay attention to any error messages Norton Antivirus may display, and write them down.

Troubleshooting help. It is possible for Norton to detect a worm, virus, or trojan that it cannot eradicate. If that occurs, Norton will indicate the virus name, and which files it could not delete. This information may be necessary for later troubleshooting.

If you run into a problem you can't resolve, call Microcomputer Services at **346-4412**

Late-breaking news: On September 10, Microsoft released a version of the RPC vulnerability patch that is newer than the one on our Security CD. *However, we recommend you run the Security CD first, then connect to the network and run Windows Update.*

Security Alerts…

Latest RPC/DCOM Worms Wreak Havoc in Record Time

W32.Wechia.Worm/Blaster attacks are wake-up call for networks worldwide

In August, two new strains of very aggressive computer worms attacked a vulnerability in Microsoft's Remote Procedure Call (RPC) implementation, replicating at record speeds and slowing networks worldwide.

W32.Welchia: This worm exploits a particular vulnerability that affects a Distributed Component Object Model (DCOM) interface with RPC that handles DCOM object activation requests sent by client machines to the server. Affected machines include Windows 2000 and Windows XP. (Linux, Macintosh, OS/2, and Unix machines are not affected).

The worm checks for active machines to infect, replicating rapidly as each infected machine continues to be a tool of the exploit. The increased network traffic Welchia generates can cause serious slow-downs—even shut-downs—of individual networks.

Resources: Complete information on W32.Welchia, including instructions for protection and removal, is available from

• CERT Advisory (CA-2003-16: Buffer Overflow in Microsoft RPC)
http://www.cert.org/advisories/CA-2003-16.html

• Symantec Security Response
http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html

• Microsoft Bulletin MS-03-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823980)
http://support.microsoft.com/default.aspx?scid=kb;en-us;823980

W32.Blaster: This worm exploits the same RPC/DCOM vulnerabilities described above, using TCP port 135. Blaster targets Windows 2000 and Windows XP machines, running code of the attacker's choice.

Resources:

• Microsoft Bulletin MS-03-039: A Buffer Overrun in RPCSS Could Allow an Attacker to Run Malicious Programs (824146)
http://support.microsoft.com/default.aspx?scid=kb;en-us;824146

• Symantec Security Response
http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html

UO Resources: UO Network Services maintains a security information page with details about the RPC/DCOM attacks on campus since July 28, 2003. See **http://security.uoregon.edu/rpcdcom/**

Important Note to UO Users: *To protect yourself against W32 variants,* ***UO Windows users should run the Microcomputer Services Security CD 2003 before connecting to UOnet****. Do* **not** *attempt to download the security patches online, because your machine will become infected before you're able to download and install the patches.*

W32.Spybot.Worm Spreads via KaZaA File Sharing and mIRC

In addition to spreading via KaZaA file sharing and mIRC (Internet Relay Chat Program), this family of worms can also spread to computers infected with common backdoor trojan viruses. The Spybot worm copies itself to the System folder of machines running Windows 95/98/NT/2000/XP/Me, and can be configured to perform a denial of service attack on specified servers or to terminate security product processes.

Macintosh, OS/2, Unix, and Linux systems are not affected.

For complete details, including security recommendations, see Symantec's Security Response page at **http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.worm.html**

Five New Microsoft Office Security Bulletins

On September 3, Microsoft released five new security bulletins, one of which was rated critical.

Four of the newly discovered vulnerabilities affect Microsoft Office desktop software. Of these, a vulnerability in Visual Basic for Applications is of most concern, as it could be exploited to gain control of a targeted PC.

The four lesser problems included a flaw in Microsoft Word and a buffer overrun in the WordPerfect converter that were rated "important," a glitch in Access's snapshot designated "moderate," and a hole in NetBIOS that was not considered significant. Despite the lesser ratings, these vulnerabilities also have potentially serious consequences.

Microsoft reiterated its advice not to open unexpected email attachments and to keep up-to-date on all patches—especially those rated "critical." For more

information on these particular vulnerabilities, see *The Register* "MS launches Office security blitz" at **http://www.theregister.co.uk/content/55/32660.html**

Get the patches. See Microsoft's Office Update page at **http://office.microsoft.com/officeupdate/**

Note that running Windows Update itself does not update Microsoft Office products! You must check for critical updates for Office separately.

Critical Flaws in IE 6 Service Pack 1, Microsoft Data Access Components

In late August, Microsoft issued two more critical updates addressing security holes in its Internet Explorer 6 Service Pack 1 and Data Access Components. Both vulnerabilities could allow attackers to compromise Windows-based systems and execute malicious code.

IE 6 Service Pack 1: This vulnerability has the potential to compromise a system with IE installed—even if IE is not used as the web browser.

Get the patch. The cumulative patch for IE 6 (**MS03-032:** August 2003 Cumulative Patch for Internet Explorer) is available from **http://support.microsoft.com/default.aspx?scid=kb;en-us;822925**

Data Access Components (MDAC): This collection of components, which provide database connectivity on Windows operating systems, is likely to be present on most Windows systems. Versions earlier than 2.8 contain the flaw.

Get the patch. You can download the patch for this vulnerability (**MS03-033:** Security Update for Microsoft Data Access Components) from **http://support.microsoft.com/default.aspx?scid=kb;en-us;823718**

Added Security for Windows 2003 Server

NGSSoftware security research breakthrough prevents stack-based buffer overflow vulnerabilities

On September 8, NGSSoftware published a paper that describes how to effectively defend against a vulnerability in Windows 2003 Server that leaves systems open to buffer overflow exploits. The paper may be downloaded from **http://www.nextgenss.com/papers/defeating-w2k3-stack-protection.pdf**

Cisco IOS Vulnerability

All Cisco devices running Cisco IOS software that are configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to denial-of-server attacks. The vulnerability is described in a July CERT Advisory (CA-2003-25:Cisco IOS Interface Blocked by IPv4 Packet) at **http://www.cert.org/advisories/CA-2003-15.html** as well as a Cisco Security Advisory (**http://cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml**)

Sendmail 8.12.10 Fixes Flaws

Installing the latest release of Sendmail fixes a known security problem and fixes other potential problems. For full details, including download information, see **http://www.sendmail.org/8.12.10.html**

A patch is also available from **http://www.sendmail.org/parse8.359.2.8.html**

Pine Vulnerabilities

On September 10, iDEFENSE (**http://www.idefense.com/**) identified two exploitable overflows in the email program Pine. Pine versions 4.56 and earlier are vulnerable. You can fix both these issues by upgrading to Pine 4.58, available from **http://www.washington.edu/pine/getpine/**

Internet Storm Center

View the locations of detected anomalies, by netblock, at **http://isc.incidents.org/source_report.html**

Seeing Spam Windows Pop Up Directly on Your PC Screen?

You may be getting hit by Messenger spam. To make it stop, see **http://www.stopmessengerspam.com/**

Repair Windows Compromises

A University of Iowa site has a comprehensive list of examples and steps for repairing Windows compromises at **http://www.its.uiowa.edu/cio/ITSecurity/documents/compromise/**

Spammers Laughing All the Way to the Bank

Last July, Amazing Internet Products' order log (inadvertently exposed by a security flaw in one of its websites) revealed that some 6000 people responded to the company's email ads and purchased penis-enlargement pills. The company grossed more than half a million dollars in one month. (For the full story on Amazing Internet Products, see the *Wired News* article, "Swollen Orders Show Spam's Allure" at **http://www.wired.com/news/business/0,1367,59907,00.html**)

A Broad Overview of Statistical Computing at

If you're new to the field of statistics, this quick overview can help get you started

Robin High
Statistical Programmer and Consultant
robinh@uoregon.edu

In recent years, the primary resources for statistical computing at the University of Oregon have been Darkwing and Oregon. Most of the statistical software on the large timesharing systems is now currently available only on Darkwing or Gladstone. Perhaps the biggest change is that statistical programs for desktop and laptop computers now have the computing edge in many situations, as I'll describe below.

What Statistical Programs Are Available?

Statistical programs for Darkwing and Gladstone. Darkwing and Gladstone are Unix-based systems for computationally intensive programs. Statistical programs available on these systems include SAS Version 8.2 and SPSS Release 6.14 (available only on Darkwing). *Note:* Although Release 6.14 is the most recent version of SPSS for Unix, it dates back to the mid-1990s and lacks some options that are available with more recent versions of SPSS that currently run on a PC or Mac.

More specialized programs. Other programs that emphasize statistical applications include SPLUS 6.1.2, BMDP 7.1, EQS, MINITAB Release 9.1, and RATS 5.01. All of these programs are available on both Darkwing and Gladstone.

SPLUS has many advanced features which more math-oriented users would feel comfortable learning. MINITAB is an interactive program that is primarily an instructional resource, and RATS is an advanced program for time series applications.

SAS is the only statistical program currently available on Oregon. Unless you have specific reasons for running SAS on this system, it is highly recommended that you to make the transition to SAS on Darkwing or a personal computer. (Note that Oregon is being phased out and will no longer be available as of fall 2004.)

For a summary of all the programs we offer, see the "Software on Darkwing and Gladstone" table on page 9. These programs are available for use by all UO students, faculty, and staff and will cover many statistical computing needs.

Statistical Programs for Personal Computers. SAS is currently the only campuswide licensed statistical software we offer for personal computers. This license allows all UO students, faculty, and staff to use SAS on campus and also load it onto personal computers at home.

SPSS for PC or Mac. Unfortunately, we're not able to offer a university-wide license for SPSS for the PC or the Mac. However, you may purchase a license directly from SPSS, obtain a valid license from your department, or run it on a computer located in a campus computing laboratory. Less expensive student versions may be an option, but some advanced procedures are not available and the program may have limited capabilities.

Other programs such as STATA and SCA may be found within specific departments, but are not officially supported at this time by the Computing Center staff.

Which Program Should You Choose?

SAS or SPSS? SAS and SPSS have long been the two primary choices for most users. Both programs handle routine analysis methods quite satisfactorily. Version 8.2 of SAS is particularly good for a broad range of statistical computing applications and is very well suited for any project that requires ongoing data file manipulations. SPSS works well for many basic statistical applications if you don't anticipate needing to continually work with data file manipulations.

Whichever program you choose, the first task is to make certain you have a valid license to run it!

In recent years the PC version of SAS has become much more versatile, powerful, and convenient to use. For members of the university community who own a computer, all it costs to acquire this software is the amount of time it takes to install (installation instructions are available at **http://sas.uoregon.edu/**).

Although PC SAS has Windows-based selection of procedures and options, its real power and versatility will be found by learning to enter commands in the editor window. Combined with the incredible computing power of PCs, you can now use SAS to run most data analysis applications typically found in classrooms or research settings. Although SAS is designed for the PC, a few MAC users have loaded and run it successfully with a PC emulator.

Running Statistical Programs

Windows interface. Statistical programs on PCs and Macs generally work with a Windows interface, either through commands submitted with a program editor or with pull-down menus.

The recommended process is to enter programs into a text editor. You can run the entire program with a "submit" command, or by highlighting a specific section with a mouse you can submit only that portion. Some

programs are interactive in that they offer a menu of choices that allow you to point-and-click your way through the analysis process (I'll have more to say on that method below.)

Batch mode. Unless you have X-Windows (e.g., Linux or the commercial product Exceed), you'd typically run statistical programs on Darkwing or Gladstone in batch mode.

Batch mode requires you to write a file of program commands with a text editor (such as pico). With this approach (known as the "syntax" method), the tasks you want the program to perform—from data input and transformations all the way to the final analysis—are clearly written into the list of program commands. Once a program is written, you submit it with a command at the system prompt.

Running a SAS Program. Darkwing and Gladstone are both case-sensitive, so to invoke a program you must enter its name in the proper case. For example, to run a SAS program on Darkwing, enter the program statements into a file called **myprog.sas** and then, at the **%** prompt, type:

```
% sas myprog
```

Note that you don't need the **.sas** extension when issuing this command.

Running a SAS program always produces an output file called **myprog.log** where you can check for error messages and summary information. When program output is produced it will be found in a file called **myprog.lst**.

Advantages of writing code with the "syntax" method. Whether you run programs on a personal computer or submit them in the batch mode, it's extremely important to keep a current record of what you did and why. Whatever software you select or system you run it on, always document your work! When you record your data processing and analysis steps in a syntax file with concise and relevant comments, this simple process can possibly save you a great deal of time and confusion in the long run.

Beware of Quick and Easy Solutions

One of the real strengths of writing program code is that it clearly documents the data analysis process. This "syntax" method is also a highly efficient way to proceed if you have many repetitive tasks or many variables to process.

The SAS Advantage. While the SAS system may seem complex (and it is), the basic statements and instructions necessary to get started are easy to learn. Once data have been read into a SAS dataset, invoking specific statistical procedures is not complicated in most cases. Also, SAS is a particularly good choice if you have data collected over time (e.g., longitudinal studies), survey data, projects that requires programming, or if you need to merge or update multiple files, among many other advantages. SAS also has a macro feature which makes repeated tasks simple to run once the basic program is written.

While "point-and-click" methods are available with many statistical programs, this approach has the potential to cause problems. Most programs do not "remember" the steps you take unless you write them or paste them to a file as you proceed. The ease of the interactive approach is appealing; however, it can cause confusion later on if you don't remember the sequence of analysis steps you took, specific options you chose, or what particular data transformations you applied. Also, it takes more time to repeat a similar or identical analysis later on. If you transfer a data file to another person, the structure or contents of the data file can be confusing if numerous variables computed over time are included. This is particularly true of SPSS for Windows, where the formulas applied are not saved in the SPSS spreadsheet (unlike EXCEL).

What about Spreadsheets?

Spreadsheet programs such as Microsoft Office's Excel are also widely available for desktop and laptop computers. While spreadsheets are strongly endorsed for data entry and storage, they are rarely suitable for statistical analyses. The choice of statistical methods is limited, and they can be very awkward to use, especially if your dataset contains many rows and columns.

Spreadsheets can compute basic summary statistics and make a few helpful graphical displays. Once your data have been entered into a spreadsheet, it's a very simple process to access them with statistical programs such as SAS or SPSS through an IMPORT procedure, direct data exchange (DDE), or saving your data in a delimited text file and having SAS or SPSS read it. More information about using Microsoft Excel as a statistics package is available at
http://www.practicalstats.com/Pages/excelstats.html

Information Resources

Workshops: Many of the concepts introduced in this article will be discussed in detail in SAS workshops this fall. Consult the IT workshop schedule (**http://libweb.uoregon.edu/it/**) for times and dates.

Web Resources: You'll find detailed information concerning statistical programs and direct connections to statistical websites at
http://darkwing.uoregon.edu/~robinh/statistics.html

For detailed product information on SAS, SPSS, and Splus, visit the vendor websites:
1. SAS: **http://www.sas.com/**
2. SPSS: **http://www.spss.com/**
3. Splus: **http://www.mathsoft.com/**

Virus Backscatter and Non-Delivery Notices for Mail You Didn't Send

These puzzling messages are most likely the effect of a computer virus

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

We've received a lot of inquiries from concerned users about "non-delivery notices" (or "email bounces") describing mail that those users didn't send, mail which was sent to people they often didn't even know.

In most cases, those messages were "backscatter" from a virus.

Having said that, it is important to understand that *you* likely didn't actually send the mail that contained the virus; a growing number of viruses forge the "From" line of the message by using addresses culled from the infested machine's address book, web page cache, or other files. (*Wired Magazine* had an excellent article on this recently; see **http://www.wired.com/news/technology/0,1282,52174,00.html**)

Obviously, these non-delivery notices for mail you didn't actually send can be very irritating, but in most cases, you should simply delete them and shrug them off as best as you can.

Many commercial Internet service providers are pretty lax when it comes to dealing with virus-infested customers, so we haven't found it very useful to forward virus reports to them.

Finally, *if* you're using a PC running some version of Windows, and even though you are likely *not* infected, please always take the following precautions:

- routinely run Windows Update from the Start button (new critical updates have been coming out literally on a weekly basis)
- make sure you've got Norton Antivirus installed and that your NAV antivirus definitions are up-to-date via LiveUpdate

Keep in mind that even though ISPs don't seem very responsive to reports of virus-ridden customers, they *do* process spam complaints—so please let us know if spam is still getting through to your Darkwing, Gladstone, or Oregon account (write to *spam@oregon.uoregon.edu*).

Pay Spammers to Stop Spamming?

Global Removal proposes novel approach to spam warfare

A new anti-spam service called Global Removal thinks Internet users are sufficiently fed up with junk email to be willing to pay a $5 lifetime fee to have their email addresses put on the company's do-not-spam list.

In a scheme some critics have compared to "paying protection money," Global proposes to pay its partners, which include more than 50 known spammers and an equal number of legitimate email marketers, to delete anti-spam subscribers' addresses from the lists they maintain.

Even being removed from these lists would not guarantee subscribers a spam-free mailbox, however; at the very least, they would still receive junk email from spammers *not* affiliated with Global.

For the full story, see the September 15 *Wired.com* article, "Anti-Spam Effort Would Pay Spammers to Stop" at **http://www.wired.com/news/business/0,1367,60431,00.html**

Google™:

It's not just a search engine, it's a calculator…

If you ever find yourself without a calculator, but with access to the web, you should know that in addition to being a search engine, Google is also a calculator.

Try it out. Say you want to subtract 933 from 1786. Go to **http://www.google.com/** and type:

1786-933=

in the search box.

For more information about this nifty Google function, see **http://www.google.com/help/features.html#calculator**

« sites worth seeing »

1. **Universities with laptop computer initiatives…** To see a current list of all the universities in the U.S. that integrate laptops into their curricula, see
   http://www.acck.edu/~arayb/NoteBookList.html
2. **Ebola Monkey Man's irreverent war on spam…** Cyber conversations designed to drive Nigerian 419 spam artists mad:
   http://www.ebolamonkeyman.com/
3. **"Flawed Routers Flood University of Wisconsin Internet Time Server"…** In May 2003, a serious flaw in hundreds of thousands of low-cost Netgear products targeted for residential use inadvertantly resulted in a denial-of-service attack on the University of Wisconsin's network. Complete details regarding the problem and its solution, including technical data, is available at
   http://www.cs.wisc.edu/~plonka/netgear-sntp
4. **Check your UO network quota online…** UO faculty, staff, and students are allotted 50MB of disk space on one of the university's large timesharing computers. To see how much space you've used and how much remains, go to
   http://password.uoregon.edu/quota/
5. **Windows XP Pro tip…** When logging into domains using Windows XP Pro, you may sometimes experience extremely long delays. You'll find tweaks and tips to fix this problem at
   http://www.windowsxpatoz.com/cgi-bin/performance/index.cgi?answer=1036283899&id=1036282433
6. **Supreme Court ruling on Internet filtering…**
   Text of the ruling:
   http://supremecourtus.gov/opinions/02pdf/02-361.pdf
   Washington Post article, "Supreme Court Upholds Internet Filters":
   http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A22519-2003Jun23&notFound=true
   Eugene *Register Guard* article, "Filtering out the filth: Eugene schools use traditional methods to block inappropriate material":
   http://www.registerguard.com/news/20020127/1a.safesurfing.0127.html
7. **"RIAA Ramps Up"…** *Washington Post* article on the growing legal war against copyrighted music filesharing.
   http://www.washingtonpost.com/wp-dyn/articles/A30875-2003Jun25.html
8. **"Patch and Pray"…** An in-depth look at the efficacy of automatically applying security patches.
   http://www.csoonline.com/read/080103/patch.html
9. **A comprehensive discussion of network security strategies…** Juniper Networks engineer Ross Callon and Cable & Wireless Chief Security Officer Bill Hancock explore the issues.
   http://www.juniper.net/company/newsletter/feature_article_030801.html
10. **"A Conversation with Jim Gray" (ACM Queue vol. 1, no. 4, June 2003) …** Fascinating interview describing the ongoing utility of "sneaker net" and the role of high capacity disk drives in moving bulk scientific data. See:
    http://www.acmqueue.org/modules.php?name=Content&pa=showpage&pid=43
11. **Inexpensive pager service available for UO business use…**
    Alphanumeric pagers for UO business use (including an unlimited number of calls per month) are available from Telecommunication Services for $4.95/month. See:
    http://www.uoregon.edu/~telcom/pager.htm

Mathematica 5.0 is Here…

In the past, Mathematica was restricted to use on campus machines, but new licensing terms for the latest version of Mathematica (5.0) now allows any UO faculty member to also install it on a personal computer at home.

Faculty members interested in running Mathematica at home should contact Hans Kuhn (*hak@uoregon.edu).*

Instructions for installing Mathematica oncampus-owned computers are available online at **http://darkwing.uoregon.edu/~hak/mathematica/**

Need help? If you have any problems with the installation process, please contact Hans Kuhn (*hak@uoregon.edu).* Questions about passwords or using Mathematica should be directed to the appropriate departmental representative. For a list of these individuals see

http://darkwing.uoregon.edu/~hak/mathematica_reps.html

Selected Elements of the 2003

Part one of a series on the evolution of university websites

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

At the request of the University of Oregon administration, we conducted a comparative study of 172 university websites this summer.

The schools selected for that study consisted of the set of all AAU universities (**http://www.aau.edu/aau/members.html**), Tier 2 or better national doctoral universities from the 2002 US News and World Report ranking (**http://www.usnews.com/usnews/edu/college/rankings/rankindex_brief.php**), and universities that have been traditional comparators or were otherwise locally nominated as being of special relevance or interest to the UO. We looked at 172 universities in all (for the complete list of universities, see **http://darkwing.uoregon.edu/~joe/2003-web-study/sites.txt**).

We summarize some of those results here because we believe they are of general interest to UO web page authors, and because they may be of interest to other universities as they think about their own websites.

Before digging into the results, we should also mention that university websites, like all websites, are frequently changed. The information we present below will obviously drift over time as various universities make incremental changes or transition to entirely new website designs.

Technical Characteristics

I. What Web Servers Are Being Used?

Every website runs on top of some sort of web server software. Choice of web server software is a fundamental one, one which can have a profound influence on factors as diverse as:

- the set of features available to page authors when building web pages
- the speed with which the web server can deliver pages to users
- the degree to which the web server can resist attacks and operate successfully in a hostile Internet-exposed networked environment
- the hardware that can be used to host that web server software (some web server software packages run only under Microsoft Windows, for example).

Comparing academic web server use to overall web server use: For the last eight years, Netcraft has been tracking global web server software market share (see **http://news.netcraft.com/**). In the latest Netcraft report, (dated August 2003 and based on their evaluation of nearly 43 million websites worldwide), Apache (**http://www.apache.org/**) was used by roughly 64% of all sites, Microsoft IIS (**http://www.microsoft.com/iis/**) was used by roughly 24%, and the remaining 12% consisted of a variety of other web server software products. This is quite comparable to the market share reported by Security Space (**http://www.securityspace.com/s_survey/data/200307**), which shows Apache at 66.6% and Microsoft at 24%, with the remainder comprising a variety of other web server software products.

In the case of our more focused study of 172 higher education web servers, we "fingerprinted" the primary web server at each of our selected sites using Internet Periscope (**http://www.lokbox.net/internetPeriscope.asp**). Of our 172 selected study sites, 121 sites (70.3%) were running Apache, 21 (12.2%) were running Microsoft IIS, and 19 (11%) were running Netscape Enterprise.

Other less popular web servers included WebStar (running at Northeastern, Reed, and the University of Connecticut), Lotus Domino (running at Seton Hall and the University of the Pacific), OSU Web Server (running at Miami University of Ohio and Ohio University), and the IBM HTTP Server (running at LSU).

A few other sites, presumably motivated by security concerns, had taken steps which made it impossible for us to fingerprint their web server software.

Some observations about the web server software results:

- The presence of Microsoft IIS is generally associated with smaller or religiously affiliated schools (e.g., Catholic University, Clark University, Fordham, Gonzaga, Pepperdine, Southern Methodist, St Thomas, SUNY ESF, Texas Christian, Yeshiva).
- Most large universities, including the University of Oregon, run Apache.
- It was somewhat surprising to see 11% of the sites in our study running Netscape Enterprise server since that web server is rather poorly represented in the larger Netcraft and Security Space studies mentioned previously. On the other hand, there is at least one study (**http://www.durak.org/sean/pubs/bss/**), focusing solely on high traffic websites, which reports a market share for Netscape that ranges from 17.6% to 25% as of June 2002, so perhaps an 11% share for Netscape Enterprise in higher education shouldn't be surprising after all.

II. Apache Modules in Use

Because Apache is modular and its base functionality can be extended via a variety of modules, we also looked to see what (if any) modules were reported as being used in conjunction with Apache. By looking at the

modules deployed, we can tell a variety of things, such as the extent to which a given website is interested in offering dynamic content, or has the ability to offer secure (encrypted) web pages from its primary server.

The most popular add-ons seen at least half a dozen of our study sites were, for the most part, the ones you'd expect to see

- **PHP** (**http://www.php.net/**) 52 study sites (43.0%) versus 52.26% for the general Internet
- **mod_ssl** (**http://www.modssl.org/**) 47 study sites (38.8%) versus 29.44 for the general Internet
- **mod_perl** (**http://perl.apache.org/**) 15 study sites (12.4%) versus 19.88% for the general Internet

(All study site percentages figured on a denominator of 121 Apache-using sites. Comparative data is from Security Space's Apache Module report for July 2003; see **http://www.securityspace.com/s_survey/data/man.200307/apachemods.html**).

The one noteworthy difference between modules in use at study sites and global trends is that while 21.92% of all global sites used the FrontPage extensions, we saw only two sites (1.6%) in our study that were running FrontPage. (There have been a variety of security issues associated with the FrontPage exceptions which may have resulted in this difference in penetration.)

Other Apache modules or add-ons seen only at a few sites included **mod_fastcgi**, **mod_pubcookie**, **DAV**, **mod_python**, **mod_layout**, **mod_auth_pam**, **mod_ldap_userdir**, **mod_macro**, **mod_jk**, **ApacheJServ**, and **mod_gzip**. For information on these or other Apache modules, see **http://modules.apache.org/**

III. Natural Web Page Size

We live in a time when there's an exceptionally wide range of screen sizes in use: everything from 640x480 (307,200 pixels) on small legacy monitors all the way up to 2048x1536 (3,145,728 pixels) on huge high resolution tubes—a full order of magnitude difference. It's difficult to design a web page that works well across that full range of resolutions.

Some sites attempt to address this issue by making their pages resizable, but doing that in a robust way can greatly complicate the page design process, and will often fail (or produce bizarre results) as users increase or decrease page size beyond relatively modest limits. The page that deserves the "gold star for near-perfect resizability," (although the design has other issues, such as its distracting use of animated page elements, that preclude giving it an unqualified thumbs up) would be New School University's site, **http://www.newschool.edu/**

Other sites simply create a fixed size page that will work on even the smallest of displays, accepting the risk that users running on large high resolution displays will see a disappointingly small (and hard to read) page; Montana State and the University of Dayton are examples of pages that take this approach. On the other hand, if you elect to optimize your web pages for larger displays, users on smaller tubes may find themselves having to scroll around in order to do even the most basic of tasks, and items which only become visible when the page is scrolled risk not being seen at all.

We were interested in what our study sites had chosen as a "natural minimum page size," or the smallest page size at which a user would not see a horizontal scroll bar appear.

The median (50th percentile) horizontal page size for our studied sites was 727.5 pixels, with an X dimension range that went from 486 pixels (University of Oklahoma) to 1229 pixels (Arizona State).

Vertically, the median page size was 717.5 pixels; the Y range extended from 409 pixels (Utah State) to 2516 pixels (the University of Kansas website, a page which stacked badly when the width of the web page was reduced down to its natural width of 625 pixels).

For comparison, the UO's natural page size is 603x694. This natural width is substantially smaller horizontally than the study sites' median width, but is right in the same ball park as Google's natural width of 571 pixels. Our height is quite close to the study median.

The images of the study websites from which these measurements were taken are available online at **http://darkwing.uoregon.edu/~joe/new-web/**

Next time…In this issue of *Computing News*, we talked about some of the mechanical issues associated with university web page delivery. In the next issue, we'll describe the trends we're seeing with respect to the actual design of higher education home pages.

Some of the university web page trends we've analyzed and will be reporting on next include:

- the battle between unified-audience and audience-segmented home page designs
- emerging approaches to handling verbose news item content on university home pages
- the *non*-portalization and *non* -animation of university home pages
- the penetration of some specific web technologies (**robots.txt** use, **favicon.ico** use, Platform for Privacy Preference (P3P) policy use, and related technologies)

Stay tuned for more on the evolution of university web sites!

industry news

SMC Produces Unmanaged Ethernet Switches with Jumbo Frame Support…for Under $200

There has been substantial interest in the Internet2 community and the IETF in increasing the Internet path MTU above the default value of 1500, either to at least 9,000 bytes (see "Practical Issues Associated with 9K MTUs" **http://darkwing.uoregon.edu/~joe/jumbos/**) or even higher still (e.g., see Matt Mathis' "Raising the Internet MTU" page at **http://www.psc.edu/~mathis/MTU/**).

Until now, a key problem has been a lack of affordable unmanaged gigabit ethernet switches with jumbo frame support for use at the workgroup level.

SMC has stepped up to the plate to fill that need, and is now offering five- and eight-port gig ethernet switches with jumbo frame support for less than $200! Wow!

For more information, see the SMC8505T and SMC8508T at **http://www.smc.com/**

AMD Opteron Processor 800 Series Available

In June, AMD announced an expansion of its product line of processors, the Opteron 800 Series.

These new processors are designed to enable enterprise as well as small and medium businesses to make an easy transition to 64-bit computing as their needs require. Innovations include an integrated memory controller and HyperTransport™ technology to increase overall performance.

For details about the new 800 series products, including pricing, see AMD's September 9 press release at **http://www.amd.com/us-en/Corporate/VirtualPressRoom/0,,51_104_543~74126,00.html**

VeriSign's Scheme to Cash in on Domain Typos Draws Fire

On September 15, VeriSign, which operates the **.com** and **.net** domain name registries, began a money-making venture to reap money from user typos—a move that wreaked havoc on many email utilities and anti-spam filters, as well as possibly violating Internet Engineering Task Force standards and VeriSign's own contract with the Internet Corporation for Assigned Names and Numbers.

In the past, a typo in a domain name lookup would simply return an error message. Under the new policy, VeriSign stands to reap advertising revenue by routing all users who misspell a domain name to VeriSign's own network of websites, instead.

Some network administrators have responded by launching technical countermeasures, reconfiguring routers and servers to block access to VeriSign's site. See:

- "VeriSign Mulls Way to Make Money from Typos" *Computer Business Review Online* 9/9/03 **http://www.cbronline.com/latestnews/d04afc52ae9da2ee80256d9c0018be8b**
- "VeriSign Looks at Earning Money on Domain Typos" *Slashdot* 9/11/03 **http://slashdot.org/article.pl?sid=03/09/11/2326205**
- "VeriSign Redirects Error Pages" *CNET 9/16/03* **http://news.com.com/2100-1032_3-5077530.html**
- Internet Software Consortium's BIND patches supporting "delegation-only" zones **http://www.isc.org/products/BIND/delegation-only.html**
- "VeriSign Sued Over Redirect Service" *CNET 9/18/03* **http://news.com.com/2100-1024-5079059.html**
- ICANN Advisory **http://www.icann.org/announcements/advisory-19sep03.htm**
- IAB Commentary **http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html**

Security Update for OpenSSH Released

On September 16, the OpenBSD Project development teams released OpenSSH 3.7.1, the latest version of the *free* Secure Shell encryption software for connecting to the Internet.

OpenSSH encrypts all network traffic (including passwords) to protect against network-level attacks such as eavesdropping and connection hijacking.

The new version supports SSH 1.3, 1.5, and 2.0 protocols and includes SFTP client and server support. It also includes other basic utilities such as **ssh-add**, **ssh-agent**, **ssh-keysign**, **ssh-keyscan**, and **ssh-keygen.**

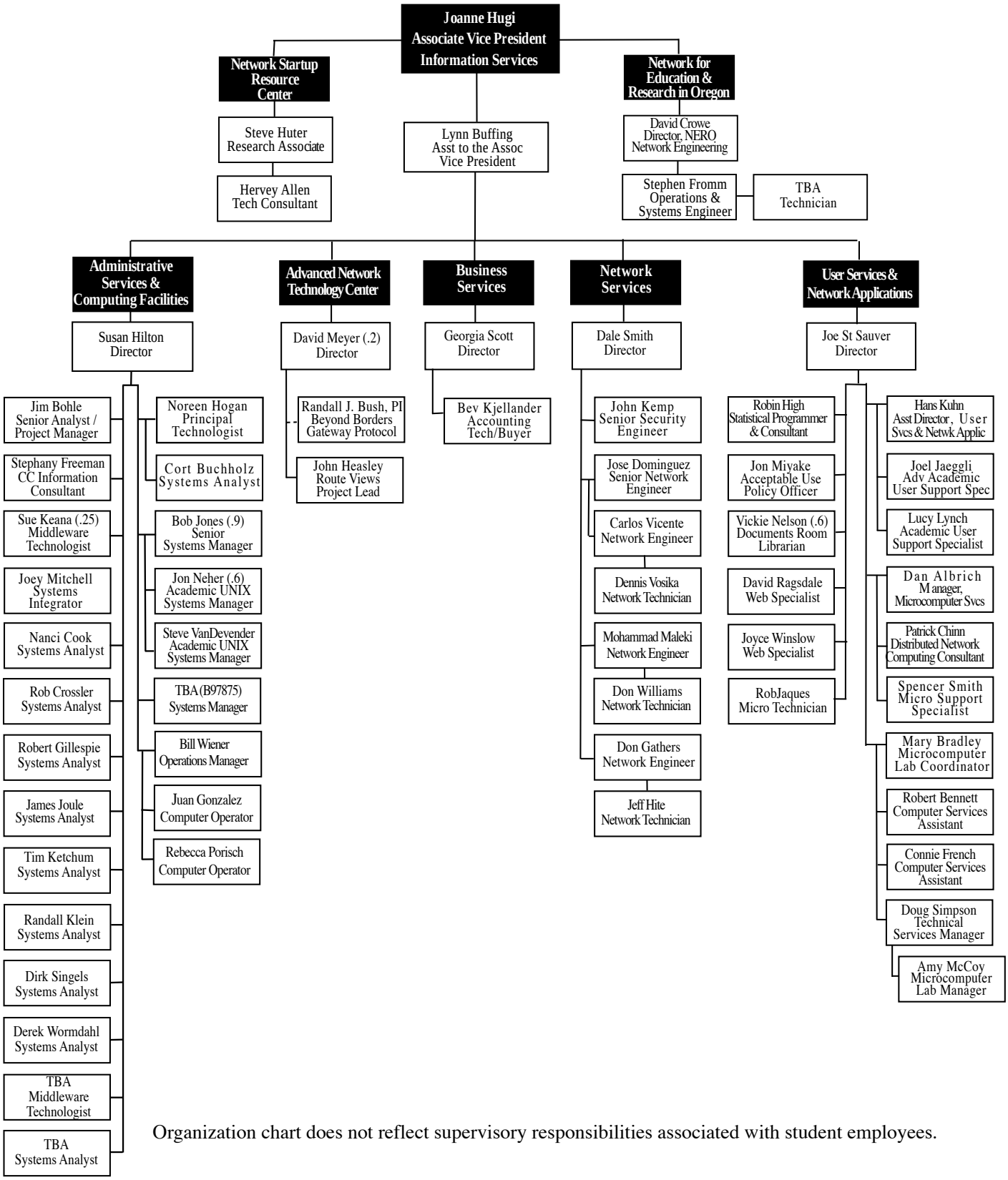
Prior to version 3.7.1., OpenSSH contained some buffer management errors. OpenSSH 3.7.1 fixes these bugs

You may download the new version by going to the OpenSSH site at **http://www.openssh.com/** and clicking on the appropriate mirror link for your system.

OpenSSH software is developed outside the U.S. using code contributed by programmers from nearly a dozen countries, and it is free to all under a BSD license.

For more information about OpenSSH, including its history and project goals, visit its website at **http://www.openssh.com/**

Computing Center Organization Chart
September 2003



Organization chart does not reflect supervisory responsibilities associated with student employees.

COMPUTING CENTER GUIDE

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

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

Microcomputer Services
http://micro.uoregon.edu/

(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, $80/hour)

346-4412
microhelp@lists.uoregon.edu

Documents Room Library
http://darkwing.uoregon.edu/~docsrm/

(175 McKenzie Hall)
346-4406

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

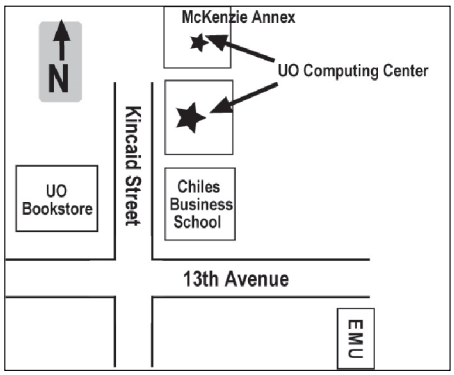
Large Systems Consulting
http://cc.uoregon.edu/unixvmsconsulting.html

(225-239 Computing Center)

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

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

Statistics Consulting
Robin High
219 Computing Center
346-1718
robinh@uoregon.edu



Electronics Shop (151 McKenzie Hall)
http://cc.uoregon.edu/e_shop.html

Computer hardware repair, installation, and upgrades.
346-3548
hardwarehelp@oregon.uoregon.edu

Network Services
http://ns.uoregon.edu/

Provides central data communication and networking services to the UO community.
346-4395
nethelp@oregon.uoregon.edu

Administrative Services
http://ccadmin.uoregon.edu/

Provides programming support for campus administrative computing, 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.

O | UNIVERSITY OF OREGON
UO COMPUTING CENTER
1212 University of Oregon Eugene, OR 97403-1212