University of Oregon

COMPUTING NEWS

SPRING 2002

Carla Meeske uses the new wireless classroom facility in Condon Hall to instruct her Marketing 199 students in Internet business basics. To find out more about the new facility, including how to reserve it for instruction, see the related article on page 11.

IN THIS ISSUE…

What's New

Features

Networking

Microcomputers

Security

Industry News Headlines

What Happens to Your UO Email Account Over the Summer?

If you're wondering whether you can use your UO account when you take a term off, read on…

If you're planning to take the summer off and return to studies this fall, will you still be able to access your UO email account?

The answer is yes, you can! All students who take a term off and then reregister for classes the following term can continue to use their computing accounts without interruption.

However, if you take *more* than one consecutive term off before reregistering, expect your account to be disabled. (Your account will be disabled during the second term in which you've failed to reregister.) This policy also applies to students who are on leave or who are involved in a program that causes them to not show current term credits for more than one term.

If you have further questions about your UO email account, or would like help setting up an automated message informing others of your new email address, call Microcomputer Services at **346-4412** or visit the Help Desk in 151 McKenzie Hall weekdays from 9 am to 5 pm.

PHP Vulnerabilities Fixed on Darkwing, Gladstone

In response to a CERT® security warning last February, Computing Center staff immediately updated PHP software on Darkwing and Gladstone to version 4.1.2.

UNIVERSITY OF OREGON

COMPUTING CENTER

COMPUTING NEWS

VOL. 17 #2

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

© University of Oregon 2002

Contact:

Joyce Winslow
jwins@oregon.uoregon.edu

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

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

Telephone: (541) 346-1724

Photography: Dave Ragsdale

PHP, a popular scripting language for dynamic websites, was first installed on Gladstone and Darkwing last fall (see the Fall 2001 *Computing News* article "Try Using PHP to Create Dynamic Web Pages…" at **http://cc.uoregon.edu/cnews/fall2001/php.html**). Early in 2002, multiple vulnerabilities were discovered that could allow hackers to execute malicious code on web servers running PHP, and system administrators were urged to upgrade to PHP 4.1.2 to avoid potential problems.

For the full text of the CERT® advisory (CA-2002-05, "Multiple Vulnerabilities in PHP fileupload"), see **http://www.cert.org/advisories/CA-2002-05.html** Another detailed discussion of the problem is available at **http://security.e-matters.de/advisories/012002.html**

If you run PHP on a server other than Darkwing or Gladstone, you may download the fix from PHP's website: **http://www.php.net/downloads.php**

Note Revised Maintenance Time for VMScluster

Rick Millhollin
Director of Computing Facilities
rickm@oregon.uoregon.edu

To make sure the UO's large timesharing computers Daisy, Donald, and Oregon are available when most users need them, scheduled weekly maintenance times on the VMScluster were revised on March 8.

Downtime on the VMScluster, which used to be on Sunday nights, now occurs on Friday nights and Sunday mornings.

The new weekly maintenance schedule (now in effect) is shown below:

Friday 7-11 pm:

The BANNER production database and associated systems like DuckWeb go down for cold backup. Oregon is not affected.

Sunday 8 -9 am:

Daisy, Donald, and Oregon all go down briefly for a cluster -wide maintenance reboot.

Got Extras?

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

Popular CC-EMU Lab Logs Heavy Use

Amy McCoy
CC-EMU Lab Manager
mccoy@oregon.uoregon.edu

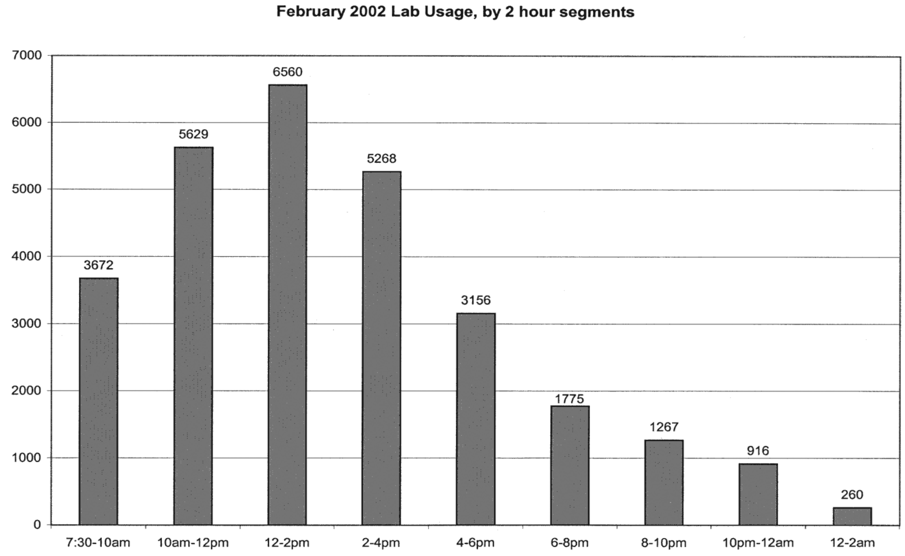
If the CC-EMU lab looked exceptionally busy to you last term, you were not hallucinating. The lab staff recently tracked their winter term traffic and came up with some interesting statistics:

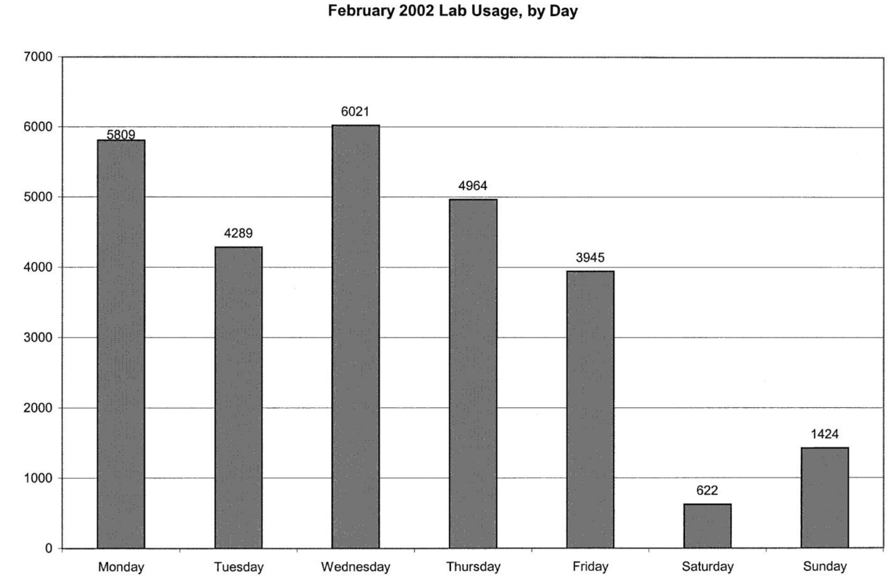
During the first two months of the year, CC-EMU lab visits totalled 53,383. This meant that, had they been used equally, each computer would have been in service 438 times.

In the month of February alone, lab visitors went through 669 reams—or 67 boxes—of paper and printed 334,369 pages on three printers.

According to February records, the busiest time of day proved to be from noon to 2 p.m., and the busiest day was Wednesday. The next most heavily trafficked day was Monday, and on every day of the week 10 a.m. to noon was runner-up for busiest time of day. Tuesday held the record for least busy weekday, and the lab was always relatively quiet for the first couple of hours after it opened at 7:30 a.m.

If the past is any measure, you can beat the crowds by studying the usage charts at right and adjusting your visits to the lab accordingly.





Check Out Micro Services' New Multimedia Equipment in 151 McKenzie

If you're interested in editing some of your digital photos or video content or converting VHS tape into digital format, check out the new multimedia equipment in 151 McKenzie.

Microcomputer Services recently upgraded its Macintosh multimedia station to include a Macintosh G4 tower with dual 1GHZ processors, 512MB RAM, an 80GB drive, a CD-R/DVD RAM combo Superdrive, and a Formac analog-to-digital converter. In addition, the station features a new Epson Perfection 2450 flatbed color image scanner with 3.3 optical density, 2400 x 4800 resolution and 48-bit color depth, and a built-in 4" x 9" transparency unit for slides, negatives, and film.

To reserve the equipment, call the Microcomputer Services help desk at **346-4412** or stop by 151 McKenzie weekdays from 9 am to 5 pm.

UO Networking Staff Participate in ICANN Meeting in Ghana

Joyce Winslow
jwins@oregon.uoregon.edu

Digital photo by Steve Huter

Joel Jaeggli (center) works with two Ghanaian technicians to distribute live Internet broadcasts of ICANN proceedings.

Last March the Internet Corporation for Assigned Names and Numbers (ICANN) held its first meeting of the year in Accra, Ghana.

The conference, the second of its kind in Africa, was hosted by Network Computer Systems (NCS) in Ghana. Two University of Oregon network specialists—Steve Huter of the Network Startup Resource Center and the Computing Center's Joel Jaeggli—were invited to help with the technical setup for the meeting. In addition to working with NCS staff to assemble the network infrastructure for the event, they also assisted in broadcasting conference sessions live on the Internet and archiving the broadcast files for future viewing.

The agenda included a variety of technical meetings for Internet service providers, domain name registrars, government advisory committees, and noncommercial constituents.

A full day was devoted to a public forum that included a discussion of ICANN President M. Stuart Lynn's proposal for a major restructuring of the organization (see related article below).

ICANN is a nonprofit organization created in 1998 to coordinate the technical management of the Internet's domain names, IP address space allocation, protocol parameters, and root server system.

Information Resources

For more information about the ICANN organization, the 2002 meeting agenda, and some of the related organizations mentioned in this article, see:

ICANN - http://www.icann.org/

ICANN Conference - http://ghana.icann.org/

NCS - http://www.ghana.com.gh/

NSRC - http://www.nsrc.org/

To locate broadcast archives from ICANN workshop sessions, see **http://videolab.uoregon.edu/events/ICANN**

Major ICANN Restructuring Proposed

The original vision of ICANN is now undergoing serious review. After nearly four years of attempting to create a purely private sector process for managing the Internet's naming and address allocation systems, some of ICANN's top officials are questioning the practicality of excluding national governments from its board.

On February 24, ICANN President M. Stuart Lynn laid out his proposals for change in a 22-page report titled "ICANN - the Case for Reform." This report, available in its entirety at **http://www.icann.org/general/lynn-reform-proposal-24feb02.htm**, outlines Lynn's reasons for abandoning ICANN's current course and urges a major restructuring of the organization. Instead of 19 board members, five of whom are elected by the general Internet community, the new board would consist of 15 members—five of them nominated by governments.

For a summary of the issues at stake in overhauling ICANN and links to other articles on the subject, see the Wired News article "If ICANN Can't, Who Should?" at **http://wired.com/news/politics/0,1283,50670,00.html**

Dealing With Pop-Up-Under Web Advertising

This intrusive type of advertising is becoming more common on the web, but there are some steps you can take to avoid it

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

If you use Yahoo or any of a growing number of other popular websites, you may have had the annoying experience of getting hit with "pop-up-under" web advertisements.

What's A 'Pop-Up-Under'?

Pop-up-under ads are stealthy, almost subliminal messages that flash across your screen when you visit a particular website. The pop-up-under scenario typically goes something like this…

You're surfing away, clicking from one web page to another. As you surf, you may have the impression that something briefly flashed on your screen, but whatever it was probably came and went so quickly you couldn't be sure. You check your screen again and don't see anything new. After a minute you rub your eyes and decide that you must have been hallucinating—but in fact, you *did* see something. What you saw was a "pop-up-under" advertisement flashing briefly across your screen before slipping behind your web browser's main window.

Once that pop-up-under hides beneath your main web page, it quietly lurks there until you close your main browser window (or move it enough to reveal the concealed pop-up-under window)…then SURPRISE! This can be quite annoying, particularly given the creepy content of some of these pop-up-under advertisements.

Pop-up-under ads are different from, but closely related to, so-called "pop-up-on-exit" advertising, which may launch a new advertising window when you attempt to leave a given website. As you may know, it is possible for unscrupulous advertising entities to "trap" you in a chain of such windows, opening a new one as fast as you close the current one, until you disable Javascript or Java, kill your browser manually, or reboot your system.

What Can You Do About Pop-Up-Under Advertisements?

There are many things you can do about pop-up-under advertisements. For example:

1. You can block the pop-ups outright by using an anti-pop-up software program such as PanicWare's free Pop-Up Stopper (**http://www.panicware.com/product_dpps.html**)

2. If you don't want to add yet another program to your system, you can simply disable Javascript, Java, Active X, and similar scripting technologies in your browser. Doing so will prevent most, if not all, pop-up advertisements, as well as blocking a variety of other real and potential vulnerabilities. To disable these scripting technologies in your browser, follow the steps described at

http://www.cert.org/tech_tips/malicious_code_FAQ.html# steps

Note: Some sites, including Blackboard, Hotmail, and some online shopping sites, may require use of Javascript, Java, or Active X; if you disable Javascript, Java, or Active X, you will not be able to use those sites.

3. Avoid websites that accept placement of pop-up-under advertising, such as Yahoo. Instead, make the effort to go to sites like Google that *do not* permit pop-up-under advertising. (See Google's no popup ad policy at **http://www.google.com/help/nopopupads.html**)

4. Don't let anyone trick you into believing that if you "just" accept cookies you'll then see fewer pop-up advertisements. You do not need to compromise your privacy—and accept being tracked online—just to regain some semblance of control over your browser. Instead, use a pop-up-under blocking program, disable Javascript, Java, or ActiveX, and avoid sites that accept pop-up advertising.

5. If you inadvertently visit a website that hits you with a pop-up-under advertisement, take a minute to write a polite complaint to the website. In particular, let the site managers know that because of their advertising policies, you'll bypass their site in the future. It's true that they have the right to run whatever advertising they want on their website, but it is equally true that you have the right to avoid that website.

6. Never, *ever* click on a pop-up-under advertising window. And it goes without saying, *never* purchase products advertised via pop-up-unders, just as you should never purchase products advertised via email spam. If you ever do respond to these ads, you'll be helping to perpetuate their continued use.

What's the UO's E-Commerce Policy?

See **http://baowww.uoregon.edu/Policy/EcommercePolicy.htm**

Virtual Private Network Services Ready for

If you're interested in using encrypted VPN services to access UOnet from off-campus, here's what you need to know…

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

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

In the old days, when all off-campus users simply dialed into the UO modem pool, UOnet was always only a phone call away. Once you were successfully dialed into one of the UO's modems from home, you were connected to UOnet just as if you were on campus, and everything worked exactly the way you expected it to. But then along came broadband high-speed home DSL and cable modem services.

DSL and cable modem services were, and are, both better and worse than using a UO dialup for off-campus access. On the one hand, DSL and cable modem service are a lot faster than dialup modems. On the other hand, because DSL and cable modem service are offered by third-party service providers rather than the university itself, when you use a DSL or cable modem service you lose your UO affiliation—i.e., the UO no longer has any way of telling that the person coming in over that cable or DSL modem service is UO faculty, staff , or student.

Because we can't identify you as affiliated with the UO, you can't use site-licensed databases, nor can you take advantage of any UO-only services such as our local news server or our outbound email servers.

Moreover, whenever you connected from a non-UO Internet service provider, some of you may have had a vague and indefinable sensation that connecting from a commercial ISP was in some way riskier or less secure than connecting directly via UOnet.

Enter VPNs…

VPNs (virtual private networks) magically fix those two problems. When you use a VPN to connect from off campus, two things happen:

1. Your PC suddenly looks to the UO, and to the world, as if it is part of UOnet. With a VPN, your PC gets a UOnet network address, just as if you were connecting from on campus, regardless of whether you're really connecting from a cable modem in Springfield or a DSL provider in Eugene.

2. *All* your network traffic, all the way from your PC back to the VPN concentrator at the UO, gets encrypted. If someone at the cable company or your DSL ISP attempts to eavesdrop on your network session, they'd get only meaningless garbage.

Who Needs VPN Software?

Anyone who connects to the UO from a cable modem or via a DSL service provider but needs to have a UO IP address to access local resources should consider using this new VPN service.

If you are connecting from an on-campus hard-wired connection or if you are dialing in to one of the UO's dialin modems, you should *not* use the VPN software.

VPN FAQs

We've answered some common questions about VPN below:

Q - **Do I *have* to use the VPN software?**

A - No, you don't. Use of the VPN software is currently discretionary—and for many users, it's not needed.

Q - **Why wouldn't I want to use VPN software everywhere, all the time, even from hardwired on-campus connections?**

A - First, you should understand that when you use a VPN, your computer has to do a lot of work encrypting your network traffic, and the overhead associated with doing that limits how fast you can go (you'll still go plenty fast, but not as fast as if you were unencrypted).

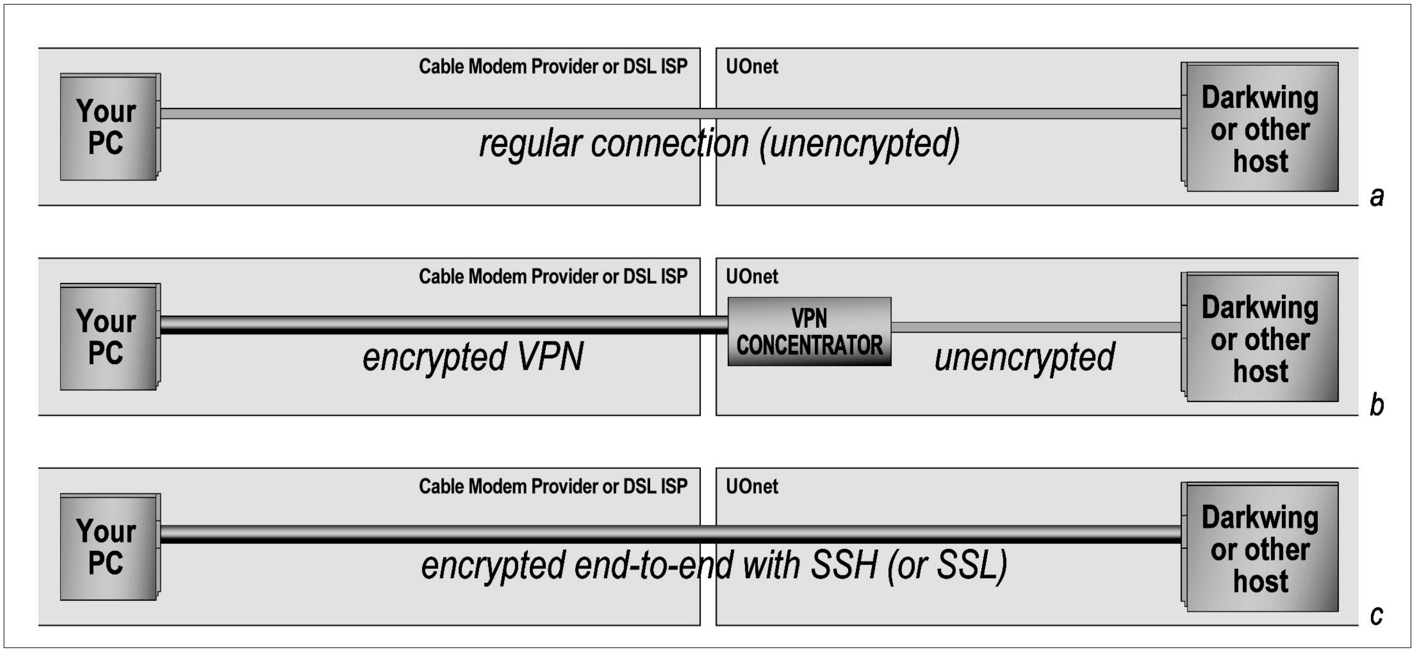
Second, using a VPN adds another level of complexity which you may want to avoid if you don't need it.

Third, you already have a UOnet address if you're connecting from on campus, so one of the VPN's big two advantages (getting a UO network address) is moot.

Q - **Even if I'm connecting from on campus, wouldn't it still be worthwhile getting the encryption that using a VPN gives me?**

A - The encryption that a VPN gives you is inferior to the

UO Off-Campus Cable Modem/DSL Users



Cable Modem Provider or DSL ISP
UOnet
Your PC
regular connection (unencrypted)
Darkwing or other host
a
Cable Modem Provider or DSL ISP
UOnet
Your PC
encrypted VPN
VPN CONCENTRATOR
unencrypted
Darkwing or other host
b
Cable Modem Provider or DSL ISP
UOnet
Your PC
encrypted end-to-end with SSH (or SSL)
Darkwing or other host
c

Diagram showing three different ways your PC can connect to networked hosts at the University of Oregon.

end-to-end encryption you get when you use ssh or when you connect to a secure web site using an SSL-enabled browser (see "c" versus "b" in the diagram above).

VPN encryption encrypts traffic from your PC running the VPN software all the way to the VPN concentrator running here on campus…but no further.

When you're using the VPN, your traffic flows over UOnet unencrypted at least part of the way, just as it does on a regular hardwired network connection from an office (see "b" versus "a" in the diagram above). Bottom line, if you're already connecting from a hardwired on-campus connection, a VPN doesn't really give you any improvement in security.

***Q* - Is this VPN the same thing as the UO Library's proxy server?**

A - No. The library's proxy service is designed solely to facilitate access to a limited set of library-purchased site licensed web-accessible online resources. If you use the VPN software, you won't need to use the library's proxy server.

***Q* - Where can I get the VPN software?**

A - The VPN software and documentation for it are available at **http://micro.uoregon.edu/getconnected**/

***Q* - How does the VPN know who I am?**

A - When you connect with the VPN, you log in with your Darkwing, Gladstone, or Oregon email address and password, which we accept as proof of who you are. (The VPN uses the same mechanism for proving who you are as our dialup modem pool.)

***Q* - Can I use other email addresses to verify my identity, such as my departmental email account on a departmentally provided email server?**

A - No, you can use only your Darkwing, Gladstone, or Oregon email address and password to authenticate.

***Q* - How do I know the VPN is actually working?**

A - The initial connection looks similar to a dialup modem connection. You'll be prompted for your username and password. Type in your full email username, including the machine address (e.g., **jersmith@gladstone.uoregon.edu**, **jersmith@darkwing.uoregon.edu**, **jersmith@oregon.uoregon.edu**). Your password is the one you use for that email account.

When you're connected, a window appears confirming you've made a successful connection. After you click "OK" on that window, a small yellow padlock icon appears in the system tray. If you double-click on the padlock icon, you'll see a window showing connection statistics and a "Disconnect" button. (You'll need to double-click on the padlock icon to end your session normally.)

***Q* - If I'm connected using the VPN, does the UO's Acceptable Use Policy apply?**

A - Yes. In particular, if you're dialed in with the VPN client, you should *not* allow family members or room-

VPN Services, continued…

mates to use your system until you disconnect from the UO VPN. Once you've disconnected from the UO VPN, what you do over your cable modem connection or DSL service is strictly a matter for you and your cable modem or DSL service provider.

Q - **Once I'm connected via the VPN, what can I access?**

A - Once you're connected via the VPN, you can access anything you could get from a regular on-campus ethernet connection, including:

- UO site-licensed online databases (such as those offered by the library)
- Online documentation limited to UO users, such as that at **http://sas.uoregon.edu/**
- UO news servers
- UO web cache servers
- UO ftp servers that are limited to UO users
- UO outgoing email (SMTP) servers
- UO's Internet2 connectivity

Q - **Will Novell IPX, AppleTalk , or IP multicast work over the VPN?**

A - The only supported protocol is TCP/IP. This means that standard applications such as web and email will work, but certain types of server connections may not. In addition, IP/TV and other multicast applications will not work through the VPN connection. If you have a particular network application that doesn't work via the UO VPN, you may wish to call us to ask for advice about possible workarounds.

Q - **How do I disconnect from the VPN?**

A -Double-click on the padlock icon in the system tray to reveal the "Disconnect" button. Click it to disconnect. Note that open network sessions will be dropped when you disconnect from the VPN.

Q - **Is there a Mac version of the VPN software?**

A - At this time, only Mac OS X is supported, and the OS X client is free. A commercial application does exist for traditional Mac OS 8/9 that you can purchase if you wish. See **http://micro.uoregon.edu/getconnected/** for details.

Q - **What If I'm Using a Linux workstation, or a Sun Sparc?**

A - A VPN client is available for both Linux and Sparc. See **ftp://ftp.uoregon.edu/vpn/3000**

I'm Confused/I Need Help!

If you're not sure if the VPN software is for you, or if you're having problems using it, feel free to contact Microcomputer Services for help. Stop by 151 McKenzie Hall weekdays any time between 9 am and 5 pm, call us at **346-4412**, or send email to *microhelp@lists.uoregon.edu*

UO Computing Conference 2002

Wednesday, May 1, 2002

Erb Memorial Union, 10 AM to 4:30 PM

FREE! Open to UO faculty, staff, and students

Troubleshooting Techniques and Tips
Introduction to PHP
Build Your Own Mass Storage Server
Windows 2000 Server
UOnet Unveiled
Security Principles
Linux Security
Discover Windows XP
Mac OS X: Your Questions Answered

To register, see http://micro.uoregon.edu/conference/
(registration limited, based on available space)

QwestDex Online Telephone Directory Debuts

Windows users can now take advantage of this paper-saving convenience

Dave Barta
Manager, Telecom Services
dbarta@oregon.uoregon.edu

Now that QwestDex's new online telephone directory is here, Windows users can browse the Eugene/Springfield directory online.

If you're using Internet Explorer (IE) or Netscape on a Windows PC, the new online directory will look much like the paper directory (see example below). Currently, only Windows machines can access the local directory, but QwestDex is reviewing options for non-Windows workstations and hopes to eventually make the product more universally available.

The Portland and Salem directories will also be available online soon.

How to Use the Directory

You can access the directory from any Windows machine on campus. If you're off-campus, you'll need a VPN connection to access it (see "VPN Access Ready…" on pp. 6-8).

First, go to

http://darkwing.uoregon.edu/qwestdex

The installer automatically determines what browser you're using and presents the appropriate installation page.

If you use IE, an icon will appear on your desktop to access the directory. For Netscape users, the application actually opens an installer which then places a small QwestDex client on your machine. Note that when installing this Netscape application, you'll be asked for a URL. This may seem confusing, but at the prompt, just type

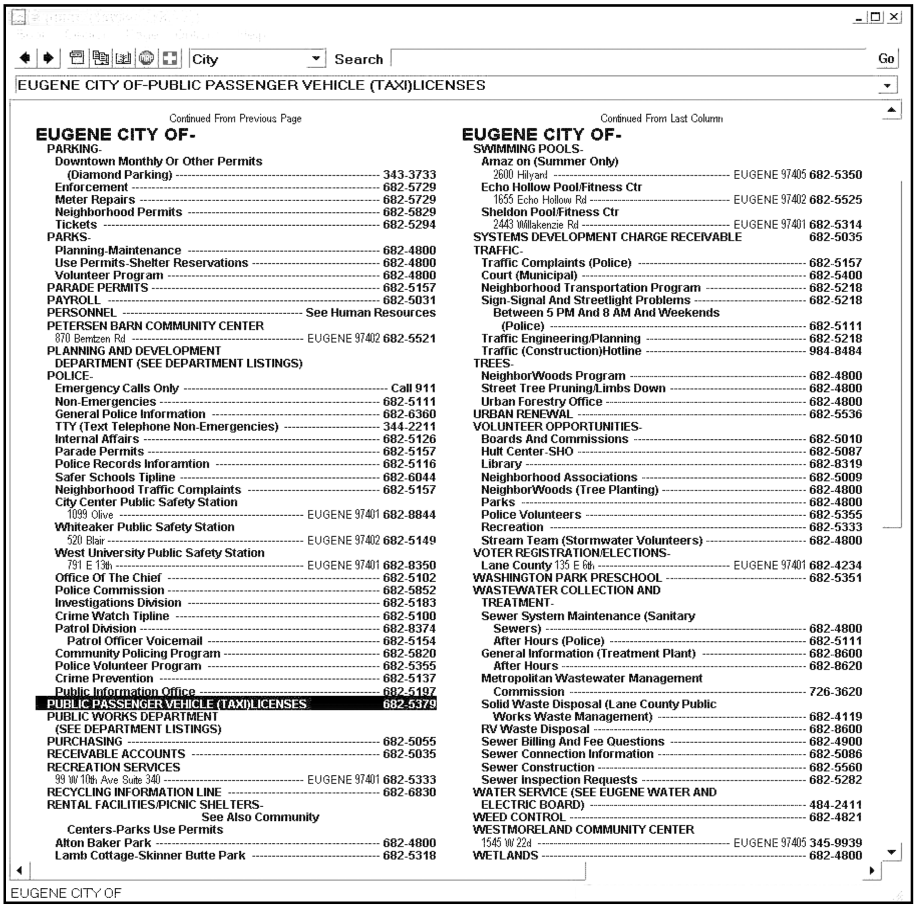
http://darkwing.uoregon.edu/qwestdex

Why Use an Online Phone Book?

QwestDex is offering UO its online directory in the hope that we'll use it instead of some or all of the roughly 5400 phone books they deliver to us every year in May. QwestDex donates the books to us free of charge, and our only expense is the cost of distributing them on campus and picking up and recycling the old ones. Our ultimate goal is to provide a useful service that conserves valuable natural resources and reduces waste. Offering the option of an online directory contributes to the conservation effort.

Alternative for non-Windows Users

Until QwestDex develops a viable solution for non-Windows users, there's another way to look up telephone numbers online that works for everyone, both on- and off-campus: just use the search engine on the QwestDex web page at **http://www.qwestdex.com**



EUGENE CITY OF-PUBLIC PASSENGER VEHICLE (TAXI)LICENSES

Continued From Previous Page

EUGENE CITY OF-

PARKING-		
Downtown Monthly Or Other Permits		
(Diamond Parking)		343-3733
Enforcement		682-5729
Meter Repairs		682-5729
Neighborhood Permits		682-5829
Tickets		682-5294
PARKS-		
Planning-Maintenance		682-4800
Use Permits-Shelter Reservations		682-4800
Volunteer Program		682-4800
PARADE PERMITS		682-5157
PAYROLL		682-5031
PERSONNEL		See Human Resources
PETERSEN BARN COMMUNITY CENTER		
870 Berntzen Rd	EUGENE 97402	682-5521
PLANNING AND DEVELOPMENT DEPARTMENT (SEE DEPARTMENT LISTINGS)		
POLICE-		
Emergency Calls Only		Call 911
Non-Emergencies		682-5111
General Police Information		682-6360
TTY (Text Telephone Non-Emergencies)		344-2211
Internal Affairs		682-5126
Parade Permits		682-5157
Police Records Inforamtion		682-5116
Safer Schools Tipline		682-6044
Neighborhood Traffic Complaints		682-5157
City Center Public Safety Station		
1099 Olive	EUGENE 97401	682-8844
Whiteaker Public Safety Station		
520 Blair	EUGENE 97402	682-5149
West University Public Safety Station		
791 E 13th	EUGENE 97401	682-8350
Office Of The Chief		682-5102
Police Commission		682-5852
Investigations Division		682-5183
Crime Watch Tipline		682-5100
Patrol Division		682-8374
Patrol Officer Voicemail		682-5154
Community Policing Program		682-5820
Police Volunteer Program		682-5355
Crime Prevention		682-5137
Public Information Office		682-5197
PUBLIC PASSENGER VEHICLE (TAXI)LICENSES		682-5379
PUBLIC WORKS DEPARTMENT (SEE DEPARTMENT LISTINGS)		
PURCHASING		682-5055
RECEIVABLE ACCOUNTS		682-5035
RECREATION SERVICES		
99 W 10th Ave Suite 340	EUGENE 97401	682-5333
RECYCLING INFORMATION LINE		682-6830
RENTAL FACILITIES/PICNIC SHELTERS- See Also Community Centers-Parks Use Permits		
Alton Baker Park		682-4800
Lamb Cottage-Skinner Butte Park		682-5318

Continued From Last Column

EUGENE CITY OF-

SWIMMING POOLS-		
Amaz on (Summer Only)		
2600 Hilyard	EUGENE 97405	682-5350
Echo Hollow Pool/Fitness Ctr		
1655 Echo Hollow Rd	EUGENE 97402	682-5525
Sheldon Pool/Fitness Ctr		
2443 Willakenzie Rd	EUGENE 97401	682-5314
SYSTEMS DEVELOPMENT CHARGE RECEIVABLE		682-5035
TRAFFIC-		
Traffic Complaints (Police)		682-5157
Court (Municipal)		682-5400
Neighborhood Transportation Program		682-5218
Sign-Signal And Streetlight Problems		682-5218
Between 5 PM And 8 AM And Weekends (Police)		682-5111
Traffic Engineering/Planning		682-5218
Traffic (Construction)Hotline		984-8484
TREES-		
NeighborWoods Program		682-4800
Street Tree Pruning/Limbs Down		682-4800
Urban Forestry Office		682-4800
URBAN RENEWAL		682-5536
VOLUNTEER OPPORTUNITIES-		
Boards And Commissions		682-5010
Hult Center-SHO		682-5087
Library		682-8319
Neighborhood Associations		682-5009
NeighborWoods (Tree Planting)		682-4800
Parks		682-4800
Police Volunteers		682-5355
Recreation		682-5333
Stream Team (Stormwater Volunteers)		682-4800
VOTER REGISTRATION/ELECTIONS-		
Lane County 135 E 6th	EUGENE 97401	682-4234
WASHINGTON PARK PRESCHOOL		682-5351
WASTEWATER COLLECTION AND TREATMENT-		
Sewer System Maintenance (Sanitary Sewers)		682-4800
After Hours (Police)		682-5111
General Information (Treatment Plant)		682-8600
After Hours		682-8620
Metropolitan Wastewater Management Commission		726-3620
Solid Waste Disposal (Lane County Public Works Waste Management)		682-4119
RV Waste Disposal		682-8600
Sewer Billing And Fee Questions		682-4900
Sewer Connection Information		682-5086
Sewer Construction		682-5560
Sewer Inspection Requests		682-5282
WATER SERVICE (SEE EUGENE WATER AND ELECTRIC BOARD)		484-2411
WEED CONTROL		682-4821
WESTMORELAND COMMUNITY CENTER		
1545 W 22d	EUGENE 97405	345-9939
WETLANDS		682-4800

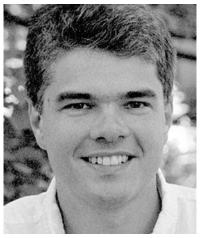
EUGENE CITY OF

The online QwestDex directory pages are formatted just as they are in the printed directory, and include the full white and yellow page listings as well as governmental listings such as the portion of a page shown above.

Smithsonian Connects to Abilene: Visit Them at http://www.si.edu

The Smithsonian Institution is a welcome new addition to the high-speed academic and research network Abilene. They're sponsored by Texas A&M and are connected through the MAX Gigapop in the Washington, D.C., area.

Should You Upgrade to Mac OS X?



Patrick Chinn
Distributed Network Computing Consultant
Microcomputer Services

pchinn@oregon.uoregon.edu

Mac OS X is a departure from previous versions of the Macintosh operating system, and new software takes time to mature. Now that Mac OS X is nearing its first birthday, some users may find that it's time to make the switch.

If you're thinking of upgrading to Mac OS X, ask yourself the following questions:

1. Do I use an iMac, iBook, PowerMac G3, PowerMac G4, PowerMac G4 cube, PowerBook G3 or PowerBook G4?

2. Do I have at least 256MB RAM?

3. Do I have, at minimum, a 6GB hard drive with 1.5GB of free space?

If you answered "yes" to all three questions, Mac OS X may be right for you. Read on to make the final determination.

If you answered "no" to one or more questions, your Macintosh will most likely not run Mac OS X in a way that's acceptable. We recommend using your current operating system until it's time to upgrade to a new computer.

To better evaluate how you use your computer, please answer these two additional questions:

4. What additional hardware (printers, scanners, cameras, external drives, etc.) do you have?

5. What software do you use regularly?

According to Apple, Mac OS X includes out-of-the-box support for most USB-compatible printers by Canon, Hewlett-Packard, and Epson, as well as most networked printers available on campus. It also supports most digital still cameras that can handle mass storage, PTP, and Digita.

We strongly recommend checking the manufacturer's web site to see if your hardware is compatible with Mac OS X. If not, assume the device will *not* work.

Software compatibility is a little less complex. Mac OS X includes a web browser and email program, and Microsoft Office is available in a Mac OS X-specific version.

Utilities like Symantec's Norton Utilities and Norton Antivirus are also available. Other popular applications, such as Adobe Photoshop, are due shortly for Mac OS X.

If there are other applications you use regularly, check Apple's Classic compatibility list (available via the link at the bottom of **http://www.apple.com/macosx/upgrade/requirements.html**) to see if the software is listed as being Classic-compatible.

Classic software loads and runs as a Mac OS 9 application within Mac OS X and does not support some of the new user interface features.

If all the software you use on a daily basis is available for Mac OS X and your computer (questions 1-3) and external hardware (question 4) are compatible, then you are ready to enter the world of Mac OS X.

Faculty and staff working in a department with in-house computer support should contact their local technical support personnel for department-specific details on running Mac OS X.

Mac OS X is available direct from Apple (**http://www.apple.com/**). Locally, it's carried by the UO Bookstore (**http://www.uobookstore.com/**). Departments may also purchase licenses through the Oregon Education Technology Consortium (**http://www.oetc.org/**).

MacNews

MacTV Brings Multimedia to Mac OS X

The latest release of MacTV, version 1.0.9, provides a way for Mac OS X users to view the university's IP/TV multicast sessions.

The application takes advantage of Mac OS X's multicast capabilities and preemptive multitasking, permitting users to continue working while the audio and video streams play.

MacTV allows users to view MPEG1, H.261 and QuickTime streams and includes an electronic program guide.

You can download MacTV from **http://www.iwitnesstv.com**

Nasty Mac OS QuickTime Exploit

If you run Mac OS 9, even if you're running it under the Classic environment in X, you're vulnerable to a QuickTime-related security hole.

The best way to protect yourself is to turn off QuickTime AutoPlay functions in the OS 9/Classic QuickTime Settings control panel—specifically, the "Enable CD-ROM Autoplay" function. It's also a good idea to rename your hard drive to something other than the default "Macintosh HD."

For details, see Ron Carlson's March 1st article "An old QT problem resurfaces as a security hole" on the IGM website at **http://www.insanelygreatmac.com/news.php?id=84** and "Auto file execution vulnerability in Mac OS" at **http://homepage.mac.com/vm_converter/mac_autoexec_vuln.html**

Facilities Services Moves Online with FAMIS Web-based Management System

Joyce Winslow
jwins@oregon.uoregon.edu

After 18 months of careful evaluation, employee training, and administrative programming adjustments, UO Facilities Services is moving its business operations online.

The software that gives the department its new web interface is the FAMIS Enterprise Facilities Management suite. FAMIS keeps track of nearly every aspect of the department's operations—including labor hours, inventory, materials purchases, billing, equipment maintenance, and projects—and interfaces seamlessly with the campus Banner finance system.

When FAMIS web modules are completely in place, all Facilities Services work will be tracked under one system, greatly streamlining operations and reducing paperwork. In addition, customers will be able to place service requests and review work order status and charges online.

The Computing Center's Administrative Services programming staff worked closely with the department to adapt FAMIS to its needs and integrate it into the campus network. Administrative Services staff also monitor the two new servers that run FAMIS, "Quince" and "Snug," which are housed in the Computing Center's central machine room.

To learn more about Facilities Services' new system, contact system administrator Sheryl Amador (*samador@darkwing.uoregon.edu*)

Facilities Services Campus Relations Manager Greta Pressman (left) congratulates Administrative Services staff members Robin Grediagin (center) and Stephany Freeman on the successful launching of FAMIS servers Quince and Snug in the Computing Center machine room. (The servers were named after two characters in Shakespeare's 'Midsummer Night's Dream.')

New Wireless Classroom Expands Teaching Options

Instructors with a yen for high tech teaching tools now have the option of using a classroom equipped with 40 wireless Dell C600 laptop computers that connect to the global Internet at ethernet speeds.

The classroom, the product of a collaboration between the UO's Classroom Improvement Committee and the Educational Technology Committee, is located on the second floor of Condon Hall in Room 204.

The spacious facility is designed with maximum flexibility in mind: tables, chairs, and laptops—even the multiple projector screens—may all be easily configured to accommodate different needs.

The computer LCD projector is compatible with a variety of modern computer platforms and its projection quality allows students to see the screen clearly even when the lights are turned on in the room. Screens are mounted from multiple locations, making it easy to project images to alternate locations.

When the laptops are not needed for instruction, they can be either locked away or closed during lectures.

The range of uses for the wireless classroom are as varied as an instructor's imagination. Students can use the laptops to gather data, to run experiments, or explore web resources, like Adjunct Instructor Carla Meeske's Marketing 199 class (see cover).

To reserve the classroom for instructional use, contact classroom scheduling at the Office of the Registrar (**346-3325**). If you plan to use the laptops for instruction, you'll also need to notify Microcomputer Lab Coordinator Mary Bradley (**346-1737**, *mbradley@oregon.uoregon.edu*) to ensure access to the equipment.

Supporting Mac OS X: Step

Making the leap from earlier Mac operating systems to Mac OS X needn't be daunting

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

Mac OS X brings countless changes for technical support personnel, and the differences between Mac OS X and its predecessors can seem overwhelming. After using and supporting Mac OS X since its days as a beta release, I've discovered that drawing on the similarities between the two operating systems makes the transition easier. To that end, this article will compare and contrast Mac OS X and its immediate predecessor, Mac OS 9.

Conventions

In prior versions of Mac OS the location of a file was noted using a path, with the colon (**:**) separating objects. Mac OS X shows its Unix underpinnings by using the forward slash (**/**) in place of the colon.

For instance, the Preferences folder in Mac OS 9 is located in **Macintosh HD:System Folder:Preferences**. In Mac OS X the system-wide Preferences files are located in **/Library/Preferences**. Note that the name of the volume is omitted in Mac OS X and included in Mac OS 9. The leading slash is meant to indicate the root of the volume, regardless of its name.

The other difference in convention is the use of the tilde character (**~**). Because each user on Mac OS X system has a folder in **/Users**, we use tilde to mean "the home directory of the user currently logged in." Since each user has his or her own folder full of preference files as well, the path is shown as **/Users/~/Library/Preferences** (Often the leading **/Users/** is omitted since the location of the user home directory does not change, leaving us with **~/Library/Preferences** in shorthand.)

BSD Unix, on which Mac OS X is built, is case and space sensitive, so watch what you type at the command prompt. File or folder names with spaces need to be enclosed with single or double quotes.

Don't Fear the CLI

CLI is short for Command Line Interface (think Unix) and is new to the Macintosh. You can issue commands using the Terminal application (found in **/Applications/Utilities**). Mac OS X does not require knowledge of Unix; you can learn most of what you need to know on the fly with the help of a good Unix reference book.

Currently, you can perform most repair and recovery functions by using a host of freeware applications available on the Internet. Many of these programs are simply GUI shells that perform command line functions. Knowing how these utilities work behind the scenes is not required, although possessing a conceptual understanding will help.

Helpful applications include Carbon Copy Cloner, which copies the Mac OS X files and user data to another volume, and Process Wizard, a menu bar/daemon combination that allows you to fine tune process priorities. These applications are available at Version Tracker: **http://www.versiontracker.com/macosx**

Startup

On startup Mac OS X loads the core operating system from the System directory. It then launches the items in **/Library/StartupItems** (This folder is analogous to Mac OS 9's "Startup Items" folder, although it's used more frequently in Mac OS X to start background processes.) After you enter your username and password, the Finder loads.

The new Finder performs much like the one in Mac OS 9. The major difference is that OS X's Finder is just another application.

No More Extensions and Control Panels

Mac OS X does not have control panels and extensions, eliminating potential concern with extension conflicts and startup crashes.

Control Panels have been replaced by preference panes, which are accessible from the Apple menu or from the Dock. Most preference panes have similar functions between the two operating systems. User-added preference panes are located in **~/Library/PreferencePanes**

Extensions have been replaced by background applications, sometimes referred to as services, processes or daemons, depending on their function. For instance, the auto-protect feature of Norton AntiVirus runs as a background process that checks for virus activity as you work.

Applications run in their own protected memory space so if one application freezes or crashes nothing else is affected. In this event, you'd simply force-quit the application (option-command-escape) and continue to work. Mac OS X versions 10.1 and later have proved to be very stable.

Going To The Library

The Library is a significant addition to Mac OS X. It is the repository for files that are system-related (fonts, preference files, ColorSync profiles) but not core system software (System, Finder, BootX). Open the Library folder and take a look around.

When applications behave badly, sometimes the cause is a damaged preferences file. The solution is to simply remove the damaged file and allow the program to create a new one. Finding preference files in Mac OS 9 was easy: they are located in the Preferences folder in the System folder.

Mac OS X handles preference files differently due to its multi-user design. System-wide preferences are stored in

by Step Approach Works Best

/Library/Preferences Each user also has his own set of preference files located in **~/Library/Preferences**

Just as in Mac OS 9, these preference files can be removed, as the application will recreate the file.

When troubleshooting preference file problems in any version of Mac OS, I recommend moving the preference file to the desktop rather than deleting it. If the file is not the source of the problem, simply drop the file back into its original storage folder.

If the Developer Tools are installed you can use the application Property List Editor to alter the contents of the preference file, a feature not available in Mac OS 9.

Internet Connections

Configuring network connections in OS X is greatly simplified compared to Mac OS 9. In X, connections are configured using the Network preference pane. Each network interface—such as Ethernet, modems, and wireless cards—has its own set of configuration tabs specific to the type of device.

In Mac OS 9, various interfaces and protocols had to be configured using a variety of control panels (e.g., AppleTalk and TCP/IP). Mac OS X pulls all of these elements together into one preference pane.

Modems and wireless cards, which require additional information to make a connection, are first configured in the Network preference pane and then later controlled by an application called "Internet Connect" (**/Applications/**).

For modem users, Internet Connect is the Remote Access control panel of Mac OS X. From here you can dial and disconnect modem connections. Internet Connect is also the place to configure Airport wireless cards.

Think "Print Center"

For printing, Apple has removed the Chooser and replaced it with Print Center, which functions much like the Desktop printer software in Mac OS 9. Print Center (located in **/Applications/ Utilities/**) creates and manages local print queues.

Non-postscript printers, mainly inkjets, require printer-specific drivers to function. Apple says that most USB-compatible printers by Epson, Hewlett-Packard, and Canon are supported out of the box. Postscript-compatible printers generally work well, but you can gain additional functionality by specifying the PPD of the particular printer you're using.

Since Mac OS X eschews AppleTalk for TCP/IP, Print Center has built-in support for printing via LPR (a fancy way of saying you can print using TCP/IP).

Mac OS X doesn't require extensive knowledge of Unix; you can learn most of what you need to know on the fly ...

Reaching the Server

As mentioned earlier, Apple has retired the Chooser. To find and log in to a server, select "Connect to a server…" from the "Go" menu. You can simply type the name of the server you wish to access or use the browser to find it.

Apple has greatly depreciated AppleTalk in Mac OS X, so the servers are not listed by AppleTalk zone. Instead, they're grouped into one large listing. Fortunately, users can add frequently-accessed servers to their favorites list.

Mac OS X also supports WebDAV (web-based storage systems like iDisk) and SMB (old-style Windows server protocol) for expanded connectivity.

Conclusion

There are many differences, large and small, between Mac OS 9 and Mac OS X. Emphasizing the similarities between the two operating systems, such as Internet Connect and Remote Access, makes Mac OS X easier to configure and support.

Oregon Rated Nation's Best for Internet Users

Oregon's laws and regulations are the e-friendliest in the nation, according to a new study by a Washington, D.C., think tank. The Progressive Policy Institute (PPI) ranked each state on the degree to which its laws and regulations encouraged e-commerce, e-government, and digital signatures. Specifically, the institute looked at how states facilitated telemedicine and online commerce. According to these criteria, Oregon was rated the "nation's best for Internet users."

For more details on the PPI's report, including how other states and regions measured up, see Dibva Sarkar's article, "Oregon rates as e-friendliest" at **http://www.fcw.com/geb/articles/2002/0311/web-ppi-03-15-02.asp**

Basic Firewall Concepts: the ABCs of

Will firewalls work for you? Find out when, where, and how to install firewalls to improve your network security.

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

As electronic security breaches increasingly become a cause for concern, a number of groups on the UO campus are recognizing a greater need for improved network security. This article focuses on one of the tools that can potentially improve network security: firewalls.

Installing a firewall requires careful consideration and planning, since a firewall is most often placed in a critical path within a network topology. This article discusses some of the most common questions that come up when considering firewall deployment, and also attempts to clarify some of the implications of introducing a firewall into a network topology.

***Disclaimer:** The topics referenced in this article are broad and complex. Volumes have been written about network security, network design, and firewall implementation. This article is merely intended to present a few of the general concepts that anyone who is contemplating a firewall installation would have to begin to address.* Building Internet Firewalls *by Zwicky, Cooper, and Chapman, is a clear and concise reference book on most of these topics, and is highly recommended.*

How Do You Know if You Need a Firewall?

The installation of a firewall requires a clear understanding of the networking requirements of a group. The installation is likely to have a direct impact on every machine behind the firewall. Since firewalls are tools used to implement network security policy, no firewall design should ever be considered without first clearly defining the ultimate security policy goals.

Risk assessment. The development of a security policy is driven by risk assessment and vulnerability analysis. A group needs to ask questions such as— "What are we trying to protect?" "Do we have anything of value on these computers?" "What would happen if we had a break- in?" If there is something of significant value on the network, then a risk assessment should be carried out. After a general risk assessment is performed, a more detailed inventory of open network services and potential vulnerabilities should follow.

It is not always the case that a firewall is the right tool for the job. If there are only a few computers within a group, then a firewall might be more than is required. Tightening host security is always a good idea, and in some cases is more than sufficient. Isolating sensitive hosts off of the network can also be a practical solution in some cases. But in general, choosing a firewall may be appropriate when there is a valuable asset that is at risk, or there are so many computers being used within a group that being sure of good host security is not possible.

What's a Good Security Policy?

A general "posture" or "stance" is usually chosen for the security policy design. This stance is used as a starting point and a conceptual framework for guiding further development of the policy. Three of the most common postures are discussed below: trust inside, least privilege, and selective blocking.

Trust inside. The most popular stance is known as "trust inside." In this scenario, it is assumed that the most significant threats will come from outside the local area network, and the emphasis of the policy will be keeping outsiders from getting in. This type of stance is frequently implemented by defining a firewall rule set that permits all connections which are initiated from the inside, but blocks connections initiated from the outside. This type of policy is easy to conceptualize and fairly easy to implement and manage.

Least privilege. Another common stance is known as "least privilege." In this stance, it is assumed that all network connections are blocked in both directions as a starting point, and the policy is incrementally opened to define precisely what is allowed. This is also known as the "deny everything" stance. Some of the individual-PC software firewalls operate in this manner, for example "ZoneAlarm Pro" and "Sygate Personal Firewall." These products force you to define firewall rules for each and every network application that is used for an outgoing connection, and also force you to define firewall rules upon receipt of new incoming connections.

Selective blocking. "Selective blocking" is another common posture. This is also known as an "accept everything" starting point. The policy is fine tuned by explicitly denying only selected connections which are known to be potentially dangerous. This is clearly the most vulnerable stance to use as a starting point. Selective blocking is often used as a first line of defense. One example is the blocking of selected incoming ports using packet filtering on a border router.

What Kinds of Firewalls are Available?

The type of firewall you choose will depend not only on the policy goals, but also on the resources available to your organization and the performance requirements of the device. Other obvious considerations are the availability of VPN software, routing and addressing features, the ease of use of the management interface, costs for sup-

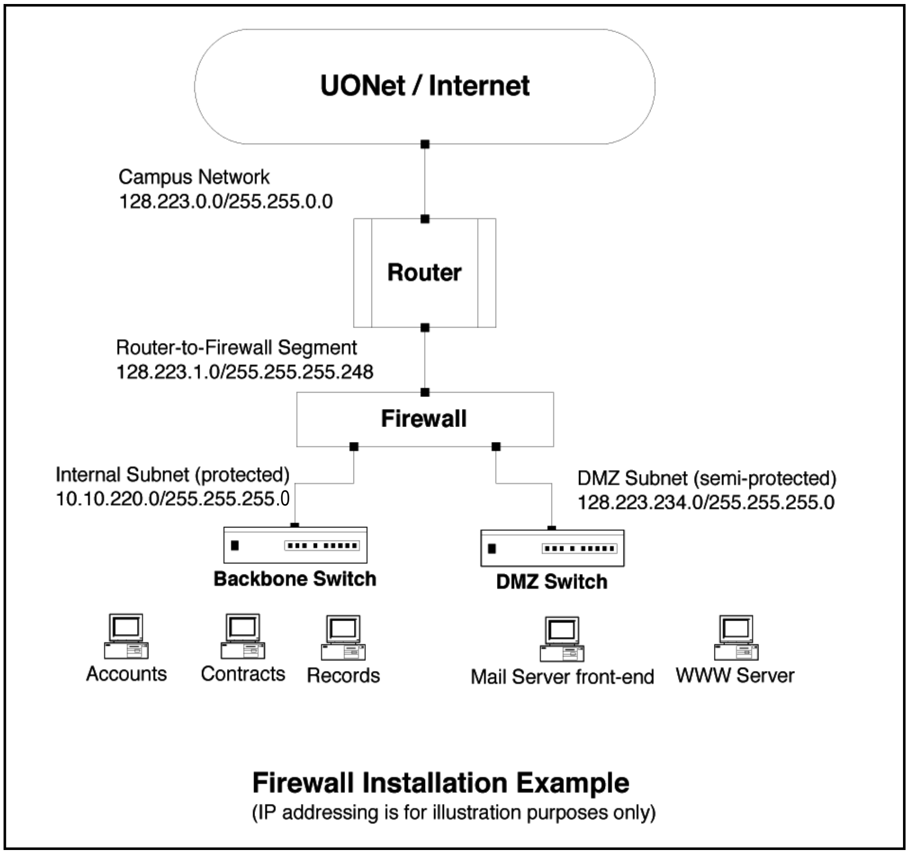


Fig. 1. Example of a firewall installation on the campus network.

port maintenance, availability of hardware redundancy, and so on.

Firewalls are typically categorized into a few types: packet filters, stateful inspection firewalls, and application proxies. Stateful inspection firewalls, which are sometimes referred to as "session-based firewalls," have become more popular in recent years. The development of hardware redundancy including session failover is a more recent feature. Every firewall product may have some or all of these general firewall capabilities.

Hardware appliances, such as the Netscreen-204, Cisco PIX 515, and Sonicwall Pro, continue to be popular because of their ease-of-use and low maintenance requirements. Since these devices do not have hard disk drives, they tend to have a high degree of hardware reliability. More expensive products, such as the Netscreen 500 and Cisco PIX 535, support higher speed interfaces at higher cost.

Do-it-yourself Unix-based firewalls running iptables, ipchains, or ipfilter, can also perform well. But the time, energy, and expertise required to develop a DIY solution can be significant. The only place where these devices seem to make sense is where there is a full-time staff member who has a good feel for the operating system being used as well as a good understanding of networking fundamentals.

There are even cases where the existing campus router for the subnet is capable of providing sufficient packet filtering to meet the needs of a group. Since routers are usually busy performing routing tasks, this kind of setup is the exception rather than the rule. But it can be an option when the policy in question is short, clear, and not subject to change.

Where is a Firewall Located?

Firewalls are typically located at the boundary between two networks. In a campus environment this border is often defined to be the department subnet.

At the University of Oregon, each department has at least one connection to one of the campus routers. This connection leads to a primary backbone switch located somewhere in the department's building. Firewalls would most often be installed in the wiring closet of the department, with the external/unprotected interface of the firewall connected to the campus router connection, and the internal/protected interface as the connection to the backbone switch (see Fig. 1 above).

Additional switches can be deployed to build up a richer environment. Switches can be placed in front of and behind the firewall to support different functionality. For example, some of the buildings on campus have dual router connections, and hot-standby protocols are used to failover in case of a router malfunction. A switch sitting in front of the firewall that is connected to both of these campus router interfaces can be used to preserve the router link redundancy.

This technique is also useful for interfacing media types. If the firewall supports only 10/100 interfaces and the router has a gigabit interface, a switch that has both gigabit and 10/100 interfaces can be used in front of the firewall to link the two devices. Switches are also often added on additional ports on the firewall to create DMZs (see "What is a DMZ?" below).

It should be clear that this kind of installation requires coordination. Great care should be taken to ensure that all necessary hardware is available at the time of installation, and that the network media types match up. Once a device is installed, it should be tested carefully for correct operation and for performance.

What is a DMZ?

Planning for the DMZ ("demilitarized zone," a perimeter network outside the

Firewalls, *continued…*

protected internal network) is a critical step that's often overlooked. A traditional firewall design—the so-called "three legged firewall"—will have an external/untrusted interface, an internal/trusted interface, and a DMZ interface (see Fig. 1 on page 13). The need for a DMZ is clear: a machine with public services, such as public web servers and mail server front ends, should go out on the DMZ.

The DMZ is a "semi-protected" zone. The rule of thumb is to assume that any machine placed on the DMZ is put at risk. The reason that this is an acceptable tradeoff is that it is much better to have a machine hacked on the DMZ than it is to have a machine hacked on the internal network. Great care should be taken so that interactions with the DMZ do not also expose the internal network.

In the absence of a DMZ, groups tend to make poor policy decisions. Without a DMZ, a group may be tempted to offer public services from machines within their trusted internal segment. This is a bad idea. One need look no further than the recent Nimda/CodeRed attacks against IIS, or the recent SSH buffer overflow vulnerabilities, to find examples of the danger of relaxing security policies for the sake of convenience. Opening ports through the firewall to the internal network should only be considered as a last resort.

Since the DMZ is dedicated to public access servers, the IP addressing scheme for the DMZ is often normal IP addressing. The size of the DMZ and the number of addresses used by the DMZ will depend on the number of servers and services that need to be presented to the outside.

Is Private Addressing Necessary?

The addressing scheme chosen for the internal/trusted interface is a critical decision that must be made well before installation begins. The traditional approach is to use private addressing on the internal/trusted network and then use NAT on the external interface of the firewall to translate the addresses of active connections so that they are routable (see Glossary in column 3).

Whether or not private addressing is used, the need for a DMZ implies that more than one security zone must be defined and maintained. In these situations the firewall acts like a router, directing traffic from one zone to the other.

It is easier to keep track of these different security zones when they fall under well-defined subnet boundaries. These boundaries can be created by splitting a subnet into parts using different length subnet masks, or by using wholly different subnet addressing. In addition, decisions have to be made on where and when public addressing or private addressing is used.

The real benefit of private addressing is that a machine that is on the internal network, when it is not actively connecting to some outside service, will be virtually invisible to the outside world. This characteristic is achieved as a consequence of the nature of connection state tables on stateful-inspection firewalls, and the fact that private addresses are not routed. This design is one of the most robust and most common.

One common complaint about internal private addressing is that renumbering of all of the machines on the internal network must take place at the time of firewall installation. Renumbering can be a daunting task, so it is best to plan ahead. Most firewalls come with a built-in DHCP server to simplify this task.

Summary

If your network group comprises a large number of computers or has valuable assets at risk, you may need to install a firewall to ensure security.

With careful assessment and planning, including choosing the security policy and type of firewall that best meet your needs, installing a firewall can go a long way toward easing your network security concerns.

Glossary

Firewall - a device used to implement a security policy between networks. A firewall has multiple network interfaces, and is typically used to create a secure boundary between untrusted external networks and trusted internal networks. The security policy defines what type of access is allowed between the connected networks.

DMZ - demilitarized zone, a perimeter network established to house public services, maintained outside of the internal/protected network. Since a DMZ will be open to allow public access to services, it is considered less secure than the internal/protected network.

Private Addresses - a specified set of IP address ranges that have been set aside for use within internal networks. These addresses begin with the following prefixes: 10.x.x.x, 192.168.x.x, and 172.16.x.x-172.31.x.x. Organizations use these addresses internally but do not forward them beyond their routers. See RFC 1597 at
http://www.nic.mil/ftp/rfc/rfc1597.txt

NAT - network address translation, a method by which IP addresses are mapped transparently from one group of addresses to another. If ports are also mapped, this may be referred to as "port address translation." NAT is often used to map a set of private/internal addresses to a smaller set of public/external addresses. See RFC 1631 at
http://www.nic.mil/ftp/rfc/rfc1631.txt

VPN - virtual private network, a secure network connection built on top of an existing public network. VPNs are used to connect remote clients or remote branch offices to local protected networks using secure encryption and authentication technologies. (See "Virtual Private Network Services Ready for UO Off-Campus…Users" on pp. 6-8).

Haunted by the Specter of Data Loss? Norton Ghost to the Rescue!

Ghost backups can protect you from catastrophic data loss

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

Anyone who has ever lost a paper, dissertation, take-home exam, or any other important file knows that backing up your hard drive is a must. At some point, your computer can—and will—die, taking all your hard work and data files with it. Recovering your files from a crashed hard drive is always tedious, often frustrating, and sometimes impossible. Once the hard drive has crashed, it often needs to be replaced, and all the applications, programs, settings, and files must be reinstalled from scratch.

How Ghost Saves You Grief

Symantec's Norton Ghost makes recovering from these catastrophic crashes easy and complete. All data, including user settings, installed applications, and files can be quickly and easily restored. Ghost creates an image of your entire drive or partition and writes that to a variety of storage media. Support for Zip disks, Jaz drives, CD-R drives, and other large-capacity storage media is built into the program.

You can also back up your drive to another internal drive or partition. (You could conceivably store your Ghost image to multiple floppy disks, but with modern operating systems alone taking up 1.5GB of storage space, you'd need a wheelbarrow for all the floppies necessary to create a backup on floppies.)

Compression. You have a choice of three levels of compression listed for the backup: None, Fast, and Small. With no compression, the Ghost image will take up the same amount of space as the used portions of the target drive, and the recovery is relatively quick. Creating a small, more compressed Ghost image will yield some space savings, but will increase both the time to create the image and the time to recover the volume. The amount of space saved depends on the predominant type of files being backed up. Applications and other binary data don't compress well, and may actually increase the size overall due to the overhead involved in compression.

Backing Up with Ghost

Caveats. Before you start, be aware that there are a few caveats involved in creating a Ghost image. Ghost works from a DOS shell and is limited to the kind of things DOS can do. For example, NTFS is not supported in the consumer-level version because it's not accessible from DOS. External USB and Firewire media are likewise not supported.

Step 1: Create a floppy. The first order of business is creating a Ghost boot floppy. All Ghost's operations are done from a booted floppy disk, running either PC-DOS or MS-DOS (if you have MS-DOS disks available). You can choose to include CD-RW support, peer-to-peer networking support, and various other drivers. (The peer-to-peer networking support does work, but this article will concentrate on the local drive options.) Pick your options in the BootWizard application and allow it to create the boot floppy.

Step 2: Secure your backup media. If you're going to use CD-R disks, you'll need to divide the total used capacity of your hard drive by 650MB, then buy that number of CD-Rs to hold the disk image. Another good option is to buy a second hard drive that's large enough to hold the used portion of your drive. IDE hard drives are relatively inexpensive these days, and a full backup on demand, inside your computer, can be invaluable. A 20GB IDE drive currently sells for less than $100, and should be adequate for an internal backup.

Step 3: Start the backup. Once your media is ready, you're all set for the backup. Boot from the Ghost floppy you've created and allow the Ghost program to boot. It will spend some time loading drivers for your mouse and keyboard and then look for CD-R drives and other devices.

At the Ghost interface, select "Local," then "Disk" (or "Partition," if your C: drive is a partition on a larger disk with multiple partitions) from the resulting pop-up window, then "To Image." A dialog box will appear, asking for the source disk or partition. Select the volume you want to back up. You'll see a "Save Filename" dialog that lists all your connected drives. Select your CD-R drive from the list. There is also an option to add a floppy disk image to the CD-R backup. Adding this floppy image allows you to boot from the backup CD without needing a floppy disk—a very handy feature.

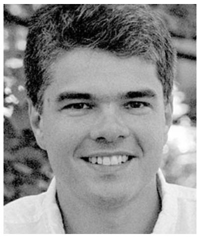
Once you select the target CD-R drive, you'll be given an option to compress the image file. If you have a large amount of data on the drive, compression can help lower the number of CDs necessary for the backup. Backing up with no compression can speed your recovery later, though. I generally choose the "Fast" compression option; this saves some space, and is relatively quick to restore.

Once you've made these selections, insert your CD-R media into the drive and allow Ghost to copy your data. A volume with 1.5GB of data took me 15 minutes to back up on a 8x Plextor CD-R drive—about what you'd expect from an 8x CD burner.

Restoring Your Disk

To restore from your backup CD set, simply boot from the Ghost floppy again (or from the first CD-ROM you created, if you chose to add the floppy image to your CD), and select Local->Image->Disk(or Partition). You'll then be able to select your CD set as the source, your disk as the destination, and restore your disk to the exact configuration that you backed up using Ghost.

Microsoft Gets Serious About



Tech giant takes steps to close security holes in its products and prevent new ones

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

In a company-wide memo issued in January, Bill Gates stressed that Microsoft must now focus on security rather than features when writing software. Some have compared this shift in strategy to turning an aircraft carrier: the process will be lengthy and the results may take time to manifest.

Last February I attended a "Microsoft Security Update" meeting in Portland to learn about the steps Microsoft has taken to improve the security of its products, and it appears that the behemoth that is Microsoft is indeed trying to change its course.

From the very early stages of product development to plugging known holes in existing products, the company is making a concerted effort to improve security.

Tightening Code Development

Rick Hattenburg, a Microsoft PSS Security Specialist, said that in February Microsoft pulled its developers from their current projects to attend a month-long series of workshops and seminars on writing secure code. Through this training they hope to reduce or eliminate common security flaws like buffer overflow exploits.

As an additional precaution, Hattenburg said that developer's code, which was formerly reviewed by only the group manager, will now undergo additional internal reviews.

Microsoft is now using Common Criteria as the basis for code and security reviews of their products (see "References" on page 19). Microsoft's Windows 2000 Professional Server and Advanced Server appear on the list of products currently under evaluation.

Closing Known Holes

Outlook and Exchange. Notorious sources of security holes, such as the Microsoft Outlook and Exchange email client and server combination, are also being tightened up. In the past, Outlook/Exchange holes allowed viruses and worms to use Outlook's address book to send copies of themselves to the addresses stored in that data file. Microsoft is taking steps to close that hole through a method called Object Model (OM) guards. With OM guards in place (in Outlook 2002, for example), Outlook will notify the user as soon as any other application attempts to send a message using data found in the address book. Users have the option to accept or deny sending the message.

Executable attachments. Microsoft has also taken steps to prevent users from opening executable attachments. Outlook categorizes attachments based on their three-character file extension. Any executable file attachment (.exe and .bat for example) is simply sequestered from the user. Other files like MS Word and MS Excel documents are presented as usual.

2000 server. On the issue of Windows 2000 server, Microsoft is also examining configuration issues for security problems. For example, past versions of Microsoft's server software shipped with nearly all services enabled by default. Worms such as Code Red and Nimda take advantage of poor default security configurations in Microsoft's IIS web server. Microsoft Security Specialist John Cho admitted that, in hindsight, this was not a smart decision and said that future versions of Windows 2000 Server will ship with most services turned off by default.

Cho also admitted that Microsoft's decision to put the IIS data directory in the system32 directory (opening the door for the common IIS Unicode exploit) was poor. Cho said that Microsoft will add the ability to locate the IIS data directory in another location, preferably another partition.

Providing Server Security Tools

Microsoft is building tools to create what it calls "baseline server security." Previously, one needed to read through pages of security alerts, download multiple software patches, and check for common security problems like blank passwords to make a Microsoft server installation secure. Many consultants earn their fees from locking down servers running Windows 2000.

Microsoft Security Tool Kit (Windows NT, 2000). Now Microsoft will automate the process and put the tools in the hands of the system administrators.

Microsoft is making available, free of charge, the Microsoft Security Tool Kit (see "References" on page 19 for the address to order this kit). Aimed at Windows NT and

Improving Security

Windows 2000, the Security Tool Kit contains utilities like HFNetChk, URLSCAN and IIS Lockdown Wizard. A reduced-feature version, called the Personal Security Advisor, is available from Microsoft's website.

Windows Update security tool for 95/98/ME. For Windows 95, 98, and ME users, Microsoft representatives say the best way to keep your computer secure is to use Windows Update (available from the Start menu) to install critical updates to your operating system.

Microsoft Office. Microsoft Office users have a similar website, although it lacks the automation of Windows Update. Office users can download product updates from the Microsoft Office Updates website (see the "References" list below).

References

MS TechNet Security home page
http://www.microsoft.com/technet/security/default.asp

MS Security Best Practices
http://www.microsoft.com/technet/security/bestprac/bestprac.asp

MS Personal Security Advisor (a web-based scan that checks your computer's security)
http://www.microsoft.com/technet/security/tools/mpsa.asp

MS Security Tool Kit
http://www.microsoft.com/security/mstpp.asp

Subscribe to Microsoft security bulletins
http://www.microsoft.com/technet/security/bulletin/notify.asp

MS Office Updates
http://office.microsoft.com/ProductUpdates/

Common Criteria
http://www.commoncriteria.org/
and
http://niap.nist.gov/cc-scheme/

Security Alert: Trojan Virus Poses as Microsoft Security Update

Another serious exploit of Microsoft Outlook's address book has recently been seen on campus.

This virus threat, which the Symantec security response team recently upgraded to a Category 3, is known variously as W32.Gibe@mm, WORM_GIBE.A, and W32/Gibe-A. It uses Microsoft Outlook and its own SMTP engine to spread, arriving in an email message disguised as a Microsoft security update. Unsuspecting users who open the attached .exe file will become infected and their systems will then be exposed to remote backdoor intrusions.

If you receive an email with content that resembles the following, ***do not open the file attached to the message***:

> **From:** Microsoft Corporation Security Center
> **Subject:** Internet Security Update
> **Message:** Microsoft Customer, this is the latest version of security update, the update which eliminates all known security vulnerabilities affecting Internet Explorer and MS Outlook/Express as well as six new vulnerabilities
>
> How to install
> Run attached file **Q216309.exe**

Because this virus purports to be a security update, some naive users may be taken in. Remember, it is *never* a good idea to open unsolicited attachments of any kind—especially executable code (.exe files).

It is also essential to keep your antivirus software updated. W32.Gibe@mm was added to the list of Norton AntiVirus LiveUpdate definitions on March 6. If you have not installed Norton AntiVirus software or activated LiveUpdate, see **http://micro.uoregon.edu/av/** for instructions.

To see Symantec's discussion of the virus, go to **http://securityresponse.symantec.com/avcenter/venc/data/w32.gibe@mm.html**

Who's Who at the

Meet some members of our staff

Joyce Winslow
jwins@oregon.uoregon.edu

Carlos Vicente
Network Engineer, Network Services

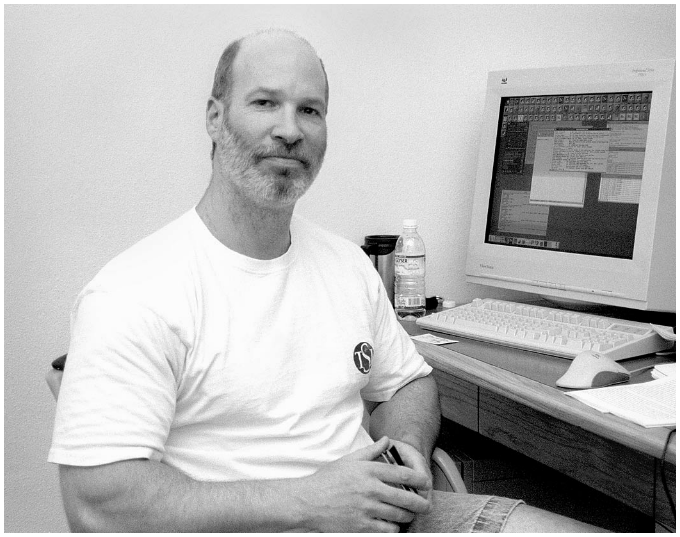
Our newest employee, Carlos Vicente, came all the way from Barcelona to join the Computing Center's Network Services staff on February 25.

Carlos' ties to the Computing Center began in 1996, when he took an undergraduate class in network engineering at Santo Domingo Institute of Technology (INTEC) in the Dominican Republic. His instructor was José Domínguez, now a senior network engineer for Network Services. Network engineering suited Carlos' talents perfectly, and he soon found himself collaborating with José to build the first academic wide-area network in the Dominican Republic. Carlos participated in every phase of the project, from installing fiber-optic cables and internal wiring to setting up servers and managing services.

This early hands-on experience served him well, and in 1999 Carlos got a scholarship to attend graduate school at the Universitat Politècnica de Catalunya in Barcelona. Studying in Spain gave him the opportunity to explore Europe a bit during the summer, and his most memorable trip was a 140-mile backpacking trek along part of the historic Camino de Santiago, a medieval pilgrimage route that runs from the Spanish/French border all the way to the city of Santiago in northeastern Spain.

After graduation Carlos worked for a short time for a Spanish Internet service provider. When the company fell victim to the dot com implosion, Carlos took advantage of an opening at the UO to rejoin his former mentor José as part of our Network Services team. One of Carlos' first assignments is to improve network management information, making router tracking and traffic engineering data more readily available for analysis. In the future he may also be called upon to oversee the UO's modem pools, managing the traffic load and troubleshooting connection problems.

While adjusting to Eugene's dreary winter weather is a challenge after a lifetime spent in sunnier climes, Carlos is looking forward to the many opportunities for outdoor adventures this area offers and plans to join the UO's Outdoor Program soon. He enjoys hiking, camping, and cycling and is also a motocross enthusiast.



Dave Meyer
Director, Advanced Network Technology Center

Dave Meyer has the sparsely furnished office of a guy constantly on the go. A half-eaten power bar teeters on the edge of his desk, a gym bag is at the ready near the door, and he keeps a big bottle of aspirin close at hand. On this particular afternoon he is dividing his attention between a ringing phone and the flickering data on his computer screen. "You're seeing a day in the life," he mutters, momentarily removing his telephone headset to hammer away at the keyboard.

This whirlwind pace is attributable to Dave's demanding dual roles as director of the UO's Advanced Network Technology Center (ANTC) and chief technologist and senior scientist for Sprint Corporation. Both jobs tap his deep experience in advanced network technologies, which has been evolving since his undergraduate days at the UO.

Dave first worked for the Computing Center in 1981, tending the campus network in its earliest incarnation. There he began what was to be the first in a long series of working collaborations with Dale Smith (now the director of Network Services). A few years later, when Dave was working on his master's degree in computer science, he joined Dale and his team of network technicians in designing and building the UO's award-winning UOnet from the ground up.

Without entirely realizing it, Dave had slipped into his life's work. Network technology was evolving exponentially, and network engineers like Dave had an opportunity to help shape the future. His specialized expertise brought him into contact with other network developers worldwide—notably Randy Bush, the founder and principal engineer of the Internet service provider RAINnet and later, director of advanced engineering at Verio and principal investigator for the Network Startup Research Center (NSRC) at the UO. Dave persuaded Randy to move RAINnet's exchange point to the UO, paving the way for innovative UO-based network solutions and collaborations that benefited education, research, and government institutions, as well as emerging networks worldwide.

In 1996, after having successfully launched OWEN/NERO (the Network for Engineering and Research in Oregon), which provides high-speed wide-area network connectivity for education and research in Oregon, Dave became director of the ANTC at the UO. Formed to promote leading-edge research, engineering, and the development of next-generation Internet protocol technologies, the ANTC oversees a number of advanced networking projects. Among these are the innovative use of IP multicast (an OWEN/NERO project), the Oregon Internet Exchange (Oregon-IX), the Oregon Gigapop connection for the high-speed Internet2 research network, and the NSRC (a project funded by a National Science Foundation grant to help support emerging network technologies in the developing world). Many of these projects involve partnerships with government agencies, national research foundations, and leading tech industries and Internet service providers.

An ANTC venture that consumes much of Dave's time these days is the Oregon Route Views Project, which provides free real-time information about global routing to Internet operators worldwide. This project has proved so successful and so useful in a variety of ways, that it is currently in the process of being expanded to meet the demand.

Over the years, Dave has crisscrossed the globe many times as a presenter and facilitator at technical conferences and workshops. When he began to forget the name of his dog, he realized it was time to cut back on travel commitments. He's now more appreciative than ever of the time he spends at home with wife Susie, daughters Rebekka (14) and Emily (20), dog Mattie, and their three cats. The Meyers' son Andy (25) is a UO journalism graduate currently pursuing a writing career in Eugene.

Dirk Singels
Systems Analyst, Administrative Services

Strictly speaking, Dirk Singels is not a native Oregonian, although he's lived in Eugene since the age of three and is a graduate of both South Eugene High and the UO.

Dirk stayed in town after high school and spent the next four years working various odd jobs, mostly at local fast-food establishments. Four years of flipping burgers convinced Dirk he'd have better career opportunities if he pursued a college education. He promptly enrolled at the UO and embarked on a course of study that earned him a B.S. in Computer Science in 1999.

Dirk immediately began work on a master's degree, paying his way with various programming jobs both on and off campus. On campus, he worked 16 hours a week for the UO Distance Education program, and Monday through Friday he commuted to northwest Eugene to write programs for MLS Internet Media. This hectic schedule inspired Dirk to interrupt his studies and "simplify his life" by working full time for a single employer. When a systems analyst position with Administrative Services opened at the Computing Center just over a year ago, Dirk promptly applied and was hired.

Like most programmers, Dirk enjoys problem solving and the satisfaction of seeing his solutions take shape in a practical way. Among his current projects are setting up new web and file servers for UO Printing Services. He is also helping to move the department's old MS-DOS-based internal accounting system to Oracle.

Dirk, who plans to eventually finish his master's program, still spends a good deal of his spare time poring over computer textbooks, and his wife Jennifer, a medical office assistant, is studying to become a registered nurse. The couple recently bought a home in Cottage Grove, so home-maintenance chores now consume most of their weekends. Despite this busy schedule, they always make time to unwind by taking long walks along Dorena Lake with Zeus, their four-year-old Doberman.

Stay on Your Toes: Security

Joyce Winslow
jwins@oregon.uoregon.edu

Despite Microsoft's resolve to tighten security in 2002 (see "Microsoft Gets Serious About Improving Security" on page 18) security flaws in Microsoft products continue to surface. This article summarizes some of the exploits reported in recent months.

Note: You can get the jump on most Microsoft vulnerabilities like the ones cited here by routinely running Windows Update. From your Start menu, go to Windows Update -> Product Updates. Pay particular attention to critical updates and service packs.

Windows/Java Security Holes

Microsoft acted quickly to fix two Java-related security problems uncovered in March. Because of their potential for harm, both these vulnerabilities were rated "critical" even though no exploits have as yet been reported and most home users will not be at risk.

Both vulnerabilities involve some versions of Java Virtual Machines (JVMs), a common application that allows Windows users to run programs written in Java. (The Microsoft VM is designed to run on the Microsoft Windows 95/98/ Me/NT 4.0/2000/XP operating systems or later.) One of these vulnerabilities could allow a malicious applet on a website to track a victim's web surfing until the browser window is closed; the other could permit malicious Java code to run outside a restricted area on your computer.

Get the fix: Microsoft's update to its JVM plugs *both* of these security holes. You may download it from **http://www.microsoft.com/java/vm/dl_vm40.htm**

Internet Software Flaws

In late February, Microsoft released patches for critical security problems with their Internet Explorer web browser and XML Core Services 2.6 (shipped with all copies of Windows XP). These problems and their solutions are briefly described below.

Internet Explorer VBScript bug. A problem with the way IE handles security for VBScripts potentially puts sensitive information, such as credit card numbers and passwords typed into a third-party web page, at risk. Because VBScript is used to access the content of other browser frames from a frame in a different domain, this glitch could be exploited to allow an attacker to read information from a victim's local drive, or from third-party web pages a user visits.

The problem affects IE 5.01, SP2, 5.5 SP1, 5.5 SP2, and 6.0.

Get the patch. The patch is available through Windows Update, as well as from **http://www.microsoft.com/windows/ie/downloads/critical/q318089/default.asp**

XML Core Services bug. This flaw occurs in an ActiveX control called XMLHTTP, which allows web pages to exchange XML data via HTTP, the standard web transfer protocol. The bug affects IE 6.0, SQL Server 2000, and all copies of Windows XP. It is similar to the IE VBScript bug, in that an attacker could gain access to a user's hard drive via malicious code imbedded in a web page, but it has several key differences. One of these is that the attacker would have to cause a user to visit a specific web page, whereas the VBScript exploit does not. Another difference is that HTML email cannot be used to carry out an attack.

For more details, see Microsoft Security Bulletin MS02-008 (on their TechNet site at **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-008.asp**).

Get the patch. The patch is available through Windows Update, as well as from **http://www.microsoft.com/windows/ie/downloads/critical/q317244/default.asp**

Mass-Mailing Worms

Two mass-mailing worms surfaced last February that take advantage of flaws in Microsoft applications. One exploits MSN Messenger, and the other sends itself to email addresses found in Microsoft Outlook addressbook and local files.

MSN Messenger worm. This worm uses Microsoft's instant messenger application to propagate and arrives in an "URGENT" message with instructions to open a link to a web page that contains malicious JavaScript code.

Variously known as "JS.Menger.Worm" and "Coolnow," the worm does no damage to the victim's site, but floods the network with the messages it propagates, sending the same message to all MSN Messenger users on the victim's contact list.

Microsoft released a "cumulative patch" for IE that fixes the flaw used by the MSN Messenger worm (see Microsoft Security Bulletin MS02-005 **at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-005.asp**), and both Symantec and F-Secure have updated their antivirus products to detect the worm.

Microsoft Outlook worm. Known as W32.Yarner.A@mm, this worm has the potential to delete all files on an affected computer. It sends messages written in German with the subject "Trojaner-Info Newsletter" and the current date.

Problems Still Plague Microsoft

The malicious attachment is named **yawsetup.exe**.

As always, a good protection against such viruses is *never* to open an unexpected attachment, especially one that contains an executable file (i.e., one with the suffix **.exe**). You should also install Norton Antivirus (included on your UO Duckware CD) and run LiveUpdate.

For full details on the W32.Yarner.A@mm worm, see **http://www.symantec.com/avcenter/venc/data/pf/w32.yarner.a@mm.html**

Server Bugs

These vulnerabilities affect the Microsoft Commerce Server 2000, SQL Server 7.0 and 2000, and Exchange 2000 server software.

Commerce Server 2000 flaw. A flaw in the server's default AuthFilter, which handles some authentication procedures, has the potential to compromise the control of your server. Attackers can exploit this flaw to launch Denial of Service (DoS) attacks that can either crash the server or run malicious code on it—in some cases, even wreaking havoc upon other computers on the network.

Get the fix. A patch will be included with Commerce Server 2000 Service Pack 3. It is also available from **http://www.microsoft.com/Downloads/Release.asp?ReleaseID=36683**

SQL Server 7.0 and 2000 vulnerabilities. These versions of SQL are vulnerable to a buffer overflow glitch that can either crash the server or give an attacker sweeping system privileges to run code on it.

Get the 7.0 fix. The patch is available from **http://support.microsoft.com/default.aspx?scid=kb;en-us;Q318268&**

Get the 2000 fix. The patch is available from **http://support.microsoft.com/default.aspx?scid=kb;en-us;Q316333&**

Exchange 2000 Server. This vulnerability could allow hackers to read or alter critical information in the server's system registry, possibly leading to an attack on the Exchange server itself.

Get the fix. Microsoft's patch for this problem is available at **http://www.microsoft.com/downloads/release.asp?ReleaseID=35462**

Telnet Glitches

Two Microsoft Telnet products, Windows 2000 Telnet Service and the Telnet Daemon in Microsoft Interix 2.2, have been found to contain unchecked buffers. This vulnerability leaves the Telnet server open to denial of service attacks and also have the potential to give hackers an opportunity to execute code on the system.

Get the Windows 2000 patch. To install the patch, you must already have Windows 2002 Service Pack 1 or 2. See **http://www.microsoft.com/windows2000/downloads/security/q307298/default.asp**

Get the Interix 2.2 patch. Go to **http://www.microsoft.com/downloads/release.asp?ReleaseID=35969**

SNMP Flaw

The Simple Network Management Protocol (SNMP) for Windows 2000 and Windows XP has security holes that could result in denial of service attacks or allow an attacker to take control of another's computer system.

For more details, and to get the patches for both Windows 2000 and XP, see Microsoft Security Bulletin MS02-006 at **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-006.asp**

Internet Explorer Holes

Cookie-Based Script Execution and Local Executable Invocation via Object Tag. At the end of March, Microsoft released a second comprehensive patch to fix two critical new security holes that surfaced in Internet Explorer 5.01, 5.5, and 6. In addition to eliminating all earlier known vulnerabilities addressed in Microsoft Security Bulletin MS02-055, this patch is intended to cover newly discovered cookie and object tag vulnerabilities and supersedes MS02-055.

Without the patch, an attacker could cause script embedded in a cookie to execute in the Local Computer Zone, or maliciously invoke an executable file already present on the user's system. For complete details, see Microsoft Security Bulletin MS02-015 at

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-015.asp

Codebase Localpath Vulnerability (IE 6). This flaw has the potential to allow attackers to shut down a computer just by getting users to visit a malicious website. As of April 1, Microsoft had not issued a patch for this flaw. Systems with the Logoff.exe or Shutdown.exe installed are particularly vulnerable. More details are available in the April 1 TechRepublic article "IE Codebase Localpath threat remains unpatched," which is available to subscribers at **http://www.techrepublic.com/**

Microsoft Security Problems, continued...

Windows NT/2000

SID filtering gap. An authentication glitch in Windows 2000 and NT 4.0 server operating systems leaves servers vulnerable to abuse by someone with administrator privileges. Because these server environments loosely allow users in one domain to access resources in another domain without strict security authentication, an attacker could extend his administrator privileges to other domains.

Microsoft offers a new security identifier (SID) filtering tool to fix this problem. See Security Bulletin MS02-001 at **http://support.microsoft.com/default.aspx?scid=kb;EN-US;q289246**

Software debugging glitch. A software debugging component of Windows 2000/NT has a security hole that can allow an attacker to take over a system without having system privileges. This hole allows any program to bypass a security gateway and initiate a debugging session

This flaw was first reported by Entercept Security Technologies and was posted on the Bugtraq security list on March 14. Microsoft has not yet released a patch, but in the meantime users can protect themselves by downloading the workaround code from
http://cert.uni-stuttgart.de/people/fw/tools/chsystem

For more details, see Sam Costello's InfoWorld article at **http://www.infoworld.com/articles/hn/xml/02/03/28/020328hnhole.xml?0329frnetworking**

Outlook 2002

Despite Microsoft's efforts to improve security in its email program, Outlook 2002 still has some problems. On March 21, Internet privacy researcher Richard Smith released a list of four vulnerabilities that make Outlook prone to virus attacks.

The problems center around email that includes HTML. One of the more critical glitches involves a special HTML tag known as an IFRAME, which has the ability to run an attached progam. Another HTML problem is the ability to run JavaScript in emails as well as read and set cookies via such email.

As of this writing, Microsoft has not yet issued technical solutions to these problems.

For more details, see Robert Lemos' article, "Just how safe is Outlook 2002?" in ZDNet News at
http://zdnet.com.com/2102-1105-866329.html

Microsoft Security References

For more information on these Microsoft security topics, see the following articles. Also note the National Security Agency recommendations for configuring Windows:

ZDNet News, Feb. 11, 2002: "MS server bugs open the door to hackers" by Matthew Broersma.
http://zdnet.com.com/2100-1104-834113.html

InfoWorld, Feb. 14, 2002: "IE flaw exploited for MSN Messenger worm" by Joris Evers.
http://www.infoworld.com/articles/hn/xml/02/02/14/020214hnworm.xml?0214alert

InfoWorld, Feb. 15, 2002: "Microsoft releases patch for SNMP flaw" by Matt Berger.
http://www.infoworld.com/articles/hn/xml/02/02/15/020215hnsnmpflaw.xml?0218mnbiznews

ZDNet News, Feb. 25, 2002: "MS warns of 'critical' flaws" by Matthew Broersma.
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,5103757,00.html

National Security Agency Windows Configuration Guides: http://nsa2.www.conxion.com/win2k/

Serious BlackICE Defender Problems with Windows 2000/XP

Ping flood vulnerability affects only Microsoft Windows 2000 and XP

If you run either BlackICE(tm) Defender 2.9 or BlackICE(tm) Defender for Server 2.9 on Microsoft Windows 2000/XP, you'll want to download the product updates right away.

The glitch allows an attacker to intentionally crash or take control of computers running this software by sending a series of packets known as a "ping flood." Product updates are available at
http://www.iss.net/support/consumer/BI_downloads.php

Did You Know?...

If you're new to campus, or even if you've been around awhile, here are some computing tips that may be useful

Did You Know You Can Create Your Own Web Pages on Darkwing, Gladstone, and Oregon?

Although many of you may think of Darkwing, Gladstone and Oregon as "where you get your email," you may not know your accounts also have space for you to create your own web pages.

To find out more about creating your own web page, see **http://cc.uoregon.edu/webpageunix.html** if your account is on Darkwing or Gladstone, or **http://cc.uoregon.edu/webpagevms.html** if you're on Oregon.

What's that "%" or "$" prompt?

With so much emphasis on the World Wide Web or client server applications such as Eudora, Fetch and WS_FTP, many users may not know they can directly "log in" to their Darkwing, Gladstone, or Oregon account and do things at the command prompt ("% " on Gladstone and Darkwing and "$" on Oregon). That process is usually called "logging on via SSH" or "working at the shell prompt."

Working at the shell prompt is quite different from using a graphical program on a PC or Mac. When you log in at the shell prompt, you actually type succinct commands and then hit Return. Text-only output appears in your ssh window.

Although Oregon's OpenVMS commands and the Unix commands used by Darkwing and Gladstone may seem a bit cryptic at first, the shell prompt is a convenience that technically inclined users often find very efficient.

Your best guide to using Unix or OpenVMS at the shell prompt is a good book. Stop by the Computing Center Documents Room Library on the ground floor of McKenzie Hall in Room 175. Documents Room staff will be happy to suggest some books that can serve as a good introduction to using Unix or OpenVMS. One particularly good introductory Unix book is Harley Hahn's *"Student's Guide to Unix*."

Is Your Email Address Listing in the Online Directory Correct?

To stay in touch with you, friends, colleagues, students, classmates, and instructors all rely on email addresses stored in the university's online directory (**http://directory.uoregon.edu/**). Please take a moment to check your address to make sure that the email address shown there is the one you routinely use.

If you see an old or incorrect address, or if you have another address that you'd simply prefer to have listed, you can change it. For information on how to change your listing, go to
http://duckweb.uoregon.edu/telecom/dir_instructions.html

Instructors: Do You Wish You Could Create a Mailing List for Your Course?

You can! See **http://lists.uoregon.edu/** for more information about managing and applying for a mailing list to use in conjunction with your course. The application form is available online at **http://lists.uoregon.edu/manage.html**

Did You Know You Can Receive Selected TV-Quality Video on Your Networked PC at the UO—and Now Even on Your Networked Mac?

Try IP/TV (for the PC), or MacTV (for Macs). To download the free client you'll need, go to
http://videolab.uoregon.edu/download.html

(If you are prompted for a "content manager" during the installation, please use **iptvhost.uoregon.edu**)

Note that some of the sessions you may see listed in the content manager may not always be available; to get started, you may want to begin by trying some of the sessions listed as "UO Presents..."

Did You Know the UO Offers Dialup Modems for Faculty, Staff and Student Use?

The UO has nearly 600 modems available for your use. To access the dialins, you'll first need an account on Darkwing, Gladstone, or Oregon. Then, go to **http://micro.uoregon.edu/getconnected/**

Note that the UO's dialin pool is designed for casual use (rather than dedicated telecommuting use, for example). The UO modems will disconnect you after two hours whether your session is busy or idle, so please watch your time while you're online to avoid surprises.

Ever Wonder How the Internet Began?

If you've ever wondered how the Internet got started, you may want to check out the book *"Where Wizards Stay Up Late: The Origins of the Internet"* by Katie Hafner and Matthew Lyon (Touchstone/Simon and Schuster, NY, 1996). It is a wonderful historical treatment of an exciting period in time.

2002 University Website Congruence Study:

Joe St Sauver, Ph.D.

Director, User Services and Network Applications

joe@oregon.uoregon.edu

It is commonly accepted and expected that most corporate websites will have a tightly controlled "look and feel." That is, all or most of the pages in a typical corporate website tend to conform to a single standard, using the same color scheme, font families, and graphical elements.

But what about university websites? Traditionally, university websites have been noteworthy for their lack of regimentation and for the diversity of styles resulting from decentralized page creation processes. But is this still true? We decided to take a systematic look...

The Home Page as Institutional Web Standard

For this study, we assumed that if a university's web pages had a standard look, that look would be most evident in its home page.

We recognize that in some cases, a university home page may incorporate features (such as periodically changing news items) that can't readily fit into a departmental website's design. However, most university home pages do exhibit common characteristics (e.g, font families, university colors, or institutional logo), which could easily be incorporated into departmental website designs.

But do academic and administrative department web pages actually incorporate those sort of elements? Is there an effort by departments to conform to a consistent institutional identity?

Eight Common Departments at Each of Seventy Universities

To check, we selected 70 major American universities. We looked at each school's home page and compared it to the primary web page ("departmental home page") for eight diverse institutional units. The eight units chosen for analysis were intentionally selected to maximize the likelihood that if diverse page designs were present (or if pages congruent with the university's home page design were present), we'd be able to see them. The eight departments we scrutinized were:

- **The English Department -** chosen as a proxy for discursive departments that might be expected to have "text heavy" page designs. English also typically represents an important mainline "Arts and Sciences" department, customarily a core academic department, with both a significant number of majors as well as service course delivery responsibilities.
- **The Art Department -** chosen as an exemplar of design-oriented departments. At many schools, web-related courses are often offered by the department—a factor which might be reflected in its web page design.
- **The Physics Department -** chosen as a typical example of numerical/analytically inclined departments (and one that might be stereotyped as being "pro-technology").
- **The Library -** selected to represent university departments with material for both on- and off-campus audiences, and a department that needs to integrate a variety of local and distributed information resources. Libraries also typically have strongly held opinions about how to best organize and deliver information to their constituencies.
- **Student Affairs -** chosen to represent a typical core administrative department present at most schools. (Cornell and Harvard didn't have traditional offices of Student Affairs)
- **Student Housing (or Residence Life) -** chosen as an example of a typically self-funded administrative department. Student Housing also taps a different dimension of institutional life in that it deals with students outside the classroom.
- **University Athletics -** college sport sites represent a highly popular visitor destination, and official university athletic sites are also of unique interest because they are often outsourced to professional web designers. Did outsourcing help or hurt overall consistency with the university's institutional motif?
- **University Alumni Office -** we believe most Alumni Offices make a concerted effort to assert their institutional affiliation by employing the university's color scheme, mascot, motifs, and so on. We also believed the Alumni Office provided another excellent example of an "outward facing" (rather than internally-oriented) web page.

Collecting the Data and Scoring the Pages

Each of those pages was visited using Netscape 4.78 on a PC running Windows 2000. We printed the pages to an HP color laser printer for scoring, and also saved screenshots of the pages captured using HyperSnap for web reference purposes.

We then scored each of the eight pages relative to each university's home page, giving each of the eight departmental pages a score ranging from 0 to 3:

- 0 = Design completely independent or unrelated to home page; an essentially incongruous design (which may incorporate a common logo, but in an inconsistent location).
- 1 = Minor or incidental resemblance to home page design; may include a common logo or other minor unifying element (used in a consistent fashion) in an otherwise not-incongruous design.
- 2 = Strong (but incomplete) resemblance to home page; incorporates some common major design elements in a not otherwise incongruous design.
- 3 = Cookie-cutter clone of home page; same or strongly similar layout with same color scheme, same font, same graphic elements—likely executed by the same designer or design team as the home page.

Each page was viewed by two scoring judges. Consensus between the judges was usually quite strong; when there

How 70 Universities Measure Up

was a difference of opinion with respect to assigned scores, discussion was used to eventually reach a consensus score. (Since we provide screen captures of the pages as they were viewed, you can easily rescore the pages yourself, if you desire to do so; see Figure 1 above.)

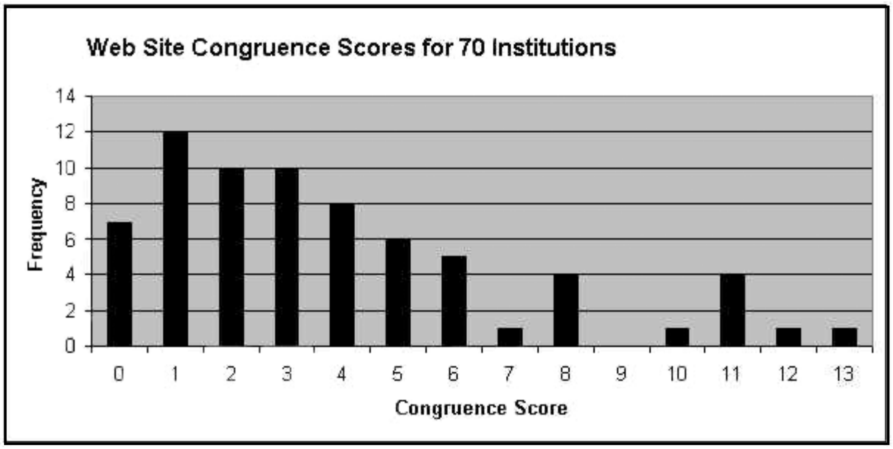


Figure 1. *Congruence scores for the websites of 70 academic institutions.*

Interpreting the Results

If all eight pages examined for a given site were closely modeled on that university's home page, the score for that institution would have been 24 (8 departments times 3 points per department). On the other hand, if all eight sample pages appeared to be independently designed and were effectively unrelated to the design of the university's home page, the score for the institution would be 0 (8 departments at 0 points per department).

Our data revealed that no school studied showed perfect design congruence (i.e., a score of 24), but ten percent of the schools examined did have scores of 11 or higher, with the University of Alaska's site having the highest overall level of congruence (with the still really quite modest score of 13).

Ten percent of the schools examined had scores of 0, indicating a high level of departmental design independence across all observed departments.

The mean total congruence score was 3.87 out of 24, with a standard deviation of 3.28. The median (50th percentile) value was 3, and the modal (most common) total congruence score was 2. The UO earned a quite typical total congruence score of 3.

Departmental Patterns

Some might wonder if particular departmental home pages were shown to be congruent with the institutional home page more often than others. Here are the patterns we found:

Departmental Congruence Score Distribution for All 70 Institutions

• English	0=50, 1=17, 2=2, 3=1
• Art	0=58, 1=10, 2=1, 3=1
• Physics	0=45, 1=19, 2=4, 3=2
• Libraries	0=53, 1=11, 2=2, 3=4
• Student Affairs	0=35, 1=20, 2=11, 3=2, N/A=2
• Sports	0=55, 9=1, 2=4, 3=2
• Housing	0=37, 1=20, 2=5, 3=8
• Alumni	0=36, 1=23, 2=8, 3=3

Looking at each of those departments, and reporting just the number of departments that had a congruence score of zero, we see the results shown in Figure 2 at the end of this article.

Thus, even in the case of administrative units such as Student Affairs and Housing, fully half the institutions in each case did not exhibit even superficial congruence between departmental home pages and the institutional home page. Clearly there is a high degree of website design autonomy across all the institutional units examined.

Conclusion

Based on the departments examined at the 70 sites studied, it is clear that universities tend to retain a significant degree of website design independence, allowing us to reject the notion that most university websites have "gone corporate." University websites continue to exhibit a refreshing degree of design autonomy and creativity, reflecting the diverse problem solving and communicative approaches commonly associated with academia.

Scores and Screen Captures

To see the web pages referenced in this study, go to "Scores and Screen Captures" at **http://darkwing.uoregon.edu/~joe/university-websites/**

To facilitate page comparisons, separate windows will open when you display individual pages.

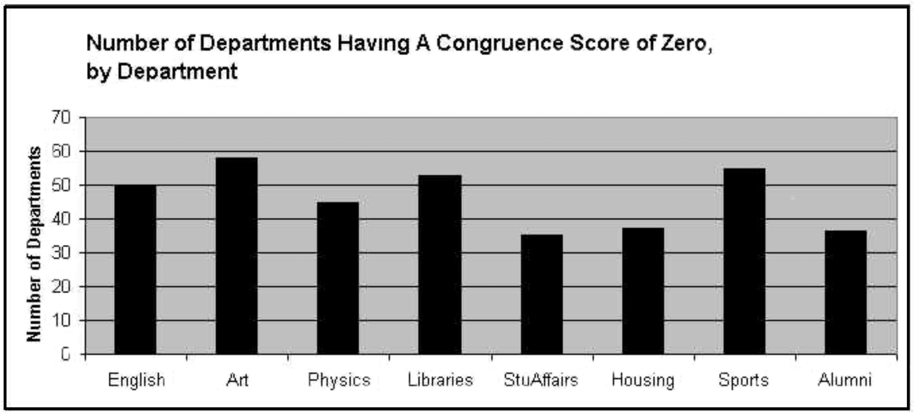


Figure 2. *Number of departments scoring zero congruence, by department.*

Asian Spam and the Fate of Spam-Ambivalent ISPs

Joe St Sauver, Ph.D.
Director, User Services and Network Applications

We've all received spam—unwanted commercial email—often touting cheap toner refills, discount Viagra (no prescription needed), online gambling opportunities, or other scams.

Recently, you may have noticed an upsurge in the amount of unreadable spam you've received—spam posted in Korean, Chinese or other non-Western character sets (such as Cyrillic). If so, you are not alone. Spam from Asia (and spam sent from North America and Europe but routed via Asian servers), has greatly increased in recent months, largely because of two factors:

1. There are a large number of systems in Korea, China, Taiwan and Russia that are vulnerable to SMTP relaying (routing email from one location—through an unrelated vulnerable system located elsewhere—to a final target located in yet a third destination). Spammers are exploiting these vulnerable Asian email systems with a vengeance.
2. Several large Korean, Chinese, Taiwanese and Russian Internet service providers have decided to allow their users to freely send spam.

In some cases these ISPs are swayed by what spammers are willing to pay them. Others are not very concerned about spamming American and European users, and simply ignore complaints.

As a result, a growing number of system administrators at sites around the world have begun to block traffic coming from particular systems that have been the source of this sort of abuse. Some ISPs (but *not* the University of Oregon), have even taken the drastic step of blocking all email from entire regions of Asia. See:

http://www.wired.com/news/politics/0,1283,50455,00.html

http://www.wired.com/news/politics/0,1283,50856,00.html

Once blocked in this way, systems may find it very difficult or impossible to get unblocked, particularly when blocking is done on a distributed basis rather than via a centrally administered, well known, and widely used blacklist.

When legitimate customers of those ISPs discover that their emails are being routinely blocked, they will have no choice but to take their business elsewhere. Being spam-friendly is a certain recipe for eventual financial failure—look what happened to AGIS in 1998 (**http://zdnet.com.com/2100-11-502030.html?legacy=zdnn**)

We mention this phenomenon to you to help you better understand why you may be seeing a large upsurge in the amount of spam from Asia, and also to encourage you to become proactive in the fight against spam. If you know any system engineers and managers at Asian ISPs, urge them to take appropriate steps to control their spam problems while there's still time.

New Resource for Web Developers…

This spring, watch for a new book on how to make your website more accessible to people with disabilities. *Constructing Accessible Websites*, published by Glasshaus, is slated to be released in April. For more details, see

http://www.glasshaus.com/html/constructing_accessible_websites/accessiblewebsites.htm

Beware: MP3 Files Can Be Written to Include Code to Launch Unwanted Web Pages

By now, nearly everyone knows that MP3 files are compressed digital music files. What you may not know is that MP3s can expose your system to attacks by unethical website operators or hackers/crackers.

Last February Bugtraq saw reports of MP3 files that could cause malicious web pages to be opened in the user's browser when an MP3 file was played. See, for example:
http://online.securityfocus.com/archive/1/258122
This exploit was also covered in ZDNet and other online news sources(**http://zdnet.com.com/2100-1104-846051.html**)

This vulnerability lies in the ability of MP3 and certain other digital music file formats to include URLs and web scripting calls. The intent behind these features was to allow synchronization of content displayed in multiple browser frames. Unfortunately, this also has the potential for abuse, such as using a music file to launch an unwanted web page—which may in turn open other unwanted pages when closed. (See "Dealing with Pop-Up-Under Web Advertising" on page 5.)

Protect yourself. The most important thing you can do is to *not* trade MP3s. MP3s you get from someone else may contain code of the sort described above (or worse). Another protective measure is to disable Javascript, Java, and ActiveX in your browser. This makes it much harder for a hacker to hijack your browser. Finally, some MP3 players may have patches designed to counter this vulnerability; make sure you've installed all available patches.

Industry News Headlines…

New Hotmail Fees

If the standard 2MB of storage space users get with their Hotmail account is not enough, they must now pay a yearly fee—plus applicable taxes—to increase their quota to 10MB.

Users who do not opt for the storage space increase may find that their messages bounce if they go over quota, and messages and attachments removed by Hotmail aren't recoverable.

Note: For security reasons, we strongly recommend that UO email account holders use SSL-encrypted UO webmail (**https://webmail.uoregon.edu**) for their web-based email instead of free web-based email such as Hotmail. Hotmail is not encrypted, leaving users vulnerable to hackers and email-borne viruses.

For more information on email security, see "UO Preferred Secure Software" at **http://micro.uoregon.edu/security/** and the article "Better Safe than Sorry…" in the Spring 2000 *Computing News* (**http://cc.uoregon.edu/cnews/spring2000/hotmailsecurity.html**).

Tiny Disc Packs 500MB Punch

DataPlay's new digital media disc is only about the size of a quarter, but it can hold either 11 hours of MP3 files, five hours of CD-quality music, or 500MB of computer data.

Four major record labels have signed up to use DataPlay technology, and the new music players are slated to be released by Samsung, Toshiba, and Matsushita in May. Retail prices are expected to range from $299 to $369. The first generation of players will be introduced with music from EMI, Universal Music Group, BMG entertainment, and Zomba Recording.

For more information on DataPlay technology, see "Small Disc Makes Big Music" at **http://www.wired.com/news/print/0,1294,51178,00.html**

Enron Shuts Down Fiber-optic Network

Fallout from the collapse of Enron Corporation has extended to its once-prized fiber-optic data network. The 18,000-mile broadband network was formerly slated to deliver video over the Internet to home subscribers through a partnership with Blockbuster. The network was turned off for several weeks in March while contracts to deliver broadband content were being assumed by a division of Dynegy Inc. and Universal Access Global Holdings.

Verizon Brings "3G" Wireless to Portland

On April 9, Verizon Wireless launched its "Taste of 3G" (third generation) high-speed Internet service in Portland. While there is some dispute whether this service is fast enough to truly be called 3G, it's still touted as the fastest wireless Internet connection in the Portland area. The new service enables customers to send email, browse the web, and download files over their wireless phone account. For more details on the new service, see:

http://www.oregonlive.com/business/oregonian/index.ssf?/xml/story.ssf/html_standard.xsl?/base/business/10184397683228688.xml

http://www.nwfusion.com/news/2002/129718_02-04-2002.html

http://www.nwfusion.com/columnists/2002/0318cooltools.html

Bell Labs Breaks Speed Record

In a recent test using DWDM (dense wave division multiplexing), Bell Labs broke the speed and distance record for transmitting data over long distances. By sending over one trillion bits of data (2.56 terabits) per second across 2500 miles, Bell nearly doubled the previous record of 1.6 terabits per second over 1250 miles.

For more details, see the Reuters report at
http://zdnet.com.com/2102-1105-867081.html

European DSL Standard Offers Higher Speeds

An emerging high-speed Internet standard in Europe could eventually replace current DSL options in the U.S. and abroad. The new G.SHDSL offers speeds that are up to three times faster than most versions of DSL targeted at business customers today, and some European communications carriers are already using it on a limited basis.

The new standard, which is capable of speeds of up to 4.6mbps, was approved by the International Telecommunication Union last February. Its data transfer speeds allow people to download and upload information at the same rate, and unlike current DSL technology, it can be made available to customers who are more than three miles away from phone company switching facilities.

For more details on G.SHDSL, see "New DSL Offers Faster Speeds" at
http://news.cnet.com/news/0-1004-200-7242800.html?tag=tp.pr

Intel Drops RDRAM

Later this year, Intel plans to drop support for Direct Rambus DRAM memory chipsets in new computer products. New chipsets supporting double data rate (DDR memory) will replace the last RDRAMs used in Xeon workstations, and Intel's new generation of workstation chipsets will support only SDRAM and DDR.

At the end of February, Intel announced its new E7500 chipset, which not only uses DDR SDRAM, but dual channel DDR SDRAM (see **http://www.ebnews.com/story/OEG20020226S0040**).

For a discussion of PC memory performance, see **http://cc.uoregon.edu/cnews/fall2000/pcmemory.html**

Network Infrastructure Companies Continue to Struggle Financially

Joe St Sauver, Ph.D.
Director, User Services and Network Applications

In a Fall 2001 *Computing News* article prepared September 5th, we stated that "for the first time major Internet infrastructure companies—companies with tangible physical assets such as fiber optic networks and network hardware devices—are also experiencing widespread financial problems." Since then, financial circumstances for major Internet carriers have not materially improved, and the following casualties have been added to the list:

- **Excite@Home** (ATHM), the broadband Internet provider, filed for Chapter 11 bankruptcy on October 1, 2001.

- **Exodus**, the major web hosting company, filed for Chapter 11 bankruptcy on September 26, 2001.

- **Genuity** (NasdaqNM:GENU), one of the largest Internet backbones, saw Standard and Poors downgrade their debt to "BB" (below investment grade) on March 15th, and shares in Genuity closed at $0.85 on April 4, 2002.

- **Global Crossing** (NYSE:GX), a major international network carrier, filed for bankruptcy on January 28 and announced on February 8 that it's being investigated by the SEC.

- **Globix** (formerly NasdaqNM:GBIX), a large web hosting company, filed for Chapter 11 bankruptcy protection on January 14, 2002.

- **McLeod** (MCLD), a facilities-based telecommunications provider with more than 31,000 route miles of fiber, filed for Chapter 11 bankruptcy protection on January 31, 2002.

- **Metromedia Fiber** (NasdaqNM: MFNX), a major metropolitan fiber network provider,is now down to $0.079/share as of 4/4/2002 after the company defaulted on several outstanding notes.

- **Nippon Telephone and Telegraph** (NYSE:NTT) announced that it expects to post the biggest loss ever by a Japanese nonfinancial company, reportedly amounting to 865 billion yen (US$6.52 billion).

- **Qwest**'s (NYSE:Q) reported $4 billion in net losses for 2001 and announced it may take accounting charges of $20 to $30 billion; it's now also under SEC investigation.

- **XO Communications** (formerly XOXO), another metro fiber network provider, reportedly said at the end of March that it may file for bankruptcy protection "in the very near future."

- **Yipes**, a facilities-based metro ethernet provider, filed for Chapter 11 bankruptcy on March 21st.

Not All the News is Bad

On the bright side, some of the financially troubled network infrastructure companies we flagged last September have successfully consolidated their operations under new ownership with minimum disruption. For example, Cable and Wireless completed its purchase of a majority of Exodus' assets this February, and PSINet has been successfully acquired by Cogent Communications. Here in Eugene, ATT Broadband has successfully migrated Excite@Home customers to its operations, while other providers have assimilated Excite@Home broadband customers in their regions.

Although so far the Internet as a whole has generally continued to perform smoothly, we urge you to remain aware of potential operational impacts of carrier financial problems.

Disclaimer: *The above market note should not be considered investment advice. If you're considering buying or selling any financial instrument, we urge you to seek qualified investment advice before proceeding.*

References

http://www.att.com/news/item/0,1847,4100,00.html
"AT&T Broadband Begins Migrating Broadband Internet Customers to New High-Speed Network"

http://www.nwfusion.com/news/2002/0201cwexodus.html
"Cable & Wireless Finalizes Purchase of Exodus"

http://biz.yahoo.com/prnews/020402/dctu045_1.html
"Cogent Communications Acquires U.S. Operations of PSINet"

http://news.com.com/2100-1033-273689.html?legacy=cnet
"Excite@Home files for bankruptcy"

http://biz.yahoo.com/rf/020315/n15251004_2.html
"Genuity Says Little Impact From S&P Downgrade"

http://news.com.com/2100-1033-824135.html
"Global Crossing Files for Bankruptcy"

http://thewhir.com/marketwatch/globix011502.cfm
"Globix Files Chapter 11, Delists from Nasdaq"

http://www.globalcrossing.com/xml/news/2002/february/08.xml
"Global Crossing Reports It Is Subject of SEC Investigation"

http://phoenix.bizjournals.com/phoenix/stories/2002/01/28/daily50.html
"McLeod files Chapter 11"

http://www.mfn.com/news/pr/20020401_MFNX.shtm
"Metromedia Fiber…Announces Senior Management Changes"

http://www.forbes.com/2002/04/04/0404ntt.html
"NTT Taking a Bath On Verio"

http://biz.yahoo.com/djus/020404/200204041915000879_1.html
"NTT Shares Open Ask-Only After Record Loss Forecast"

http://biz.yahoo.com/djus/020404/200204040333000138_5.html
"Japan's NTT Warns of Huge Loss …"

http://news.com.com/2100-1033-873388.html
"Qwest Under Fire From SEC"

http://www.qwest.com/about/media/pressroom/1,1720,951_archive,00.html
"Qwest…Notified of Formal Order of Investigation From SEC"

http://www.qwest.com/about/media/pressroom/1,1720,950_archive,00.html
"Qwest Announces Potential …Write-Down of $20-$30 Billion…"

http://cc.uoregon.edu/cnews/fall2001/ispfinances.html
"Volatile Market Conditions Affect Network Infrastructure Companies"

http://biz.yahoo.com/rf/020401/financial_xo_6.html
"XO Future Hangs in Balance"

http://story.news.yahoo.com/news?tmpl=story&u=/cn/20020325/tc_cn/
"Yipes Files For Chapter 11 Bankruptcy"

SPRING WORKSHOPS

The Library and Computing Center are committed to making sure you have opportunities to build your technology skills. Toward that end, we provide a wide range of computer and Internet training, from novice to advanced skill levels. These information technology ("IT") workshops are free and open to currently enrolled students, as well as staff and faculty.

There is no registration; all seating is available on a first-come, first-served basis. **Unless otherwise indicated , prerequisites are required.** You *must* meet the workshop prerequisites as stated in the description.

Requests for accommodations related to disability should be made to **346-1925** at least one week in advance of the workshop. For more information, contact the Office of Library Instruction (**346-1817**, *cbell@darkwing.uoregon.edu*, **http://libweb.uoregon.edu/instruct**).

THE SUMMER WORKSHOP SCHEDULE WILL BE AVAILABLE IN EARLY JUNE

This schedule is subject to change. See *http://libweb.uoregon.edu/it/* for course outlines/materials and the most current information.

Web Publishing, Multimedia ✔ Prerequisites

Workshop	Day/Date	Time	Location	Presenter
Web Publishing I - ★✔*Prerequisites:* Familiarity with a graphical web browser like Netscape or Internet Explorer and an account on Darkwing or Gladstone (not Oregon!); you must know your username and password				
	Fri Apr 19	10 - 11:50am	144 Knight Library	Johnson
	Mon Apr 22	2 - 3:50pm	144 Knight Library	Michel
	Thu May 2	10 - 11:50am	144 Knight Library	Frantz
Web Publishing II - ★✔*Prerequisites:* Web Publishing I or equivalent knowledge and skills, and a web page you've created				
	Mon Apr 29	2 - 3:50pm	144 Knight Library	Nesselroad
	Thu May 9	10 - 11:50am	144 Knight Library	Benedicto
Web Publishing III -★ ✔ *Prerequisites:* Web Publishing II or equivalent knowledge and skills				
	Thu May 16	10 - 11:50am	144 Knight Library	Bell
Dreamweaver I ✔*Prerequisite:* Web Publishing I & II or equivalent knowledge and skills				
	Thu May 23	10 - 11:50am	144 Knight Library	Smith
Dreamweaver II ✔*Prerequisite:* Web Publishing III and Dreamweaver I or equivalent knowledge and skills				
	Thu May 30	10 - 11:50am	144 Knight Library	Johnson

Communications and Research Software ✔ Prerequisites

Workshop	Day/Date	Time	Location	Presenter
EndNote/ProCite Use these programs to organize and retrieve your citations and format your footnotes and bibliographies				
	Mon Feb 4	3- 4:20pm	235 Knight Library	Lenn
	Tue Feb 5	3 - 4:20pm	235 Knight Library	Lenn
Linking Directly to Full-text Articles in Library Databases ✔*Prerequisite:* Basic knowledge of web page creation preferred				
	Wed May 15	2 - 3:30pm	144 Knight Library	Michel
PowerPoint Basics (Applicable to both Windows and Macintosh)				
	Wed Apr 17	2 - 3:50pm	144 Knight Library	Heerema
More PowerPoint ✔*Prerequisite:* PowerPoint Basics or equivalent knowledge and skills				
	Wed May 8	2 - 3:50pm	267B Knight Library	Heerema
Net a Job: Use the Web! ✔*Prerequisite:* Familiarity with a graphical web browser				
	Thu May 9	3:30 - 4:50pm	144 Knight Library	Haynes
PsycINFO ✔*Prerequisite:* Familiarity with a graphical web browser				
	Mon Apr 8	3:30 - 4:20pm	144 Knight Library	Benedicto
	Tue Apr 9	3:30 - 4:20pm	144 Knight Library	Benedicto
	Thu Apr 11	3:30 - 4:20pm	144 Knight Library	Benedicto
	Fri Apr 12	3:30 - 4:20pm	144 Knight Library	Benedicto
New! **Web of Science** Learn how to use this new database to maximize your research efforts in the sciences or social sciences				
	Tue May 14	4 - 4:50pm	235 Knight Library	Hannon, Jenkins
	Wed May 22	4 - 4:50pm	235 Knight Library	Hannon, Jenkins

★ Requires an active account on Darkwing or Gladstone

COMPUTING CENTER GUIDE

UO Website

http://www.uoregon.edu/

Computing Center Website

http://cc.uoregon.edu/

Microcomputer Services

(151 McKenzie Hall)

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

346-4412

microhelp@oregon.uoregon.edu

http://micro.uoregon.edu/

Documents Room Library

(175 McKenzie Hall)

346-4406

http://darkwing.uoregon.edu/~docsrm

Large Systems Consulting

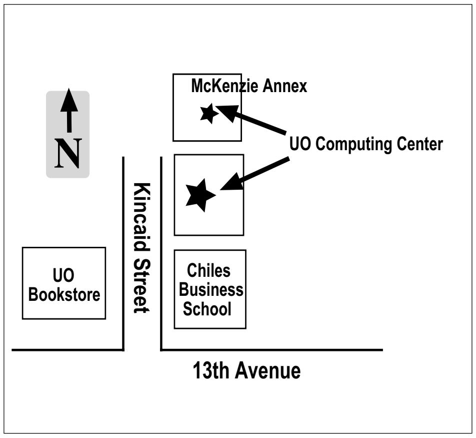
(Rooms 225-239 Computing Center)

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

346-1758

consult@darkwing.uoregon.edu
consult@gladstone.uoregon.edu
consult@oregon.uoregon.edu

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



Electronics Shop (151 McKenzie Hall)

For computer hardware repair, installation, and upgrade services, call **346-3548** or write *hardwarehelp@oregon.uoregon.edu* Also see ***http://cc.uoregon.edu/e_shop.html***

Network Services

Provides central data communication and networking services to the UO community.

346-4395

nethelp@oregon.uoregon.edu

http://ns.uoregon.edu/

Administrative Services

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

Modem Number

Dial-in modem number for UOnet, the campus network: **225-2200**

Computing Center Hours

Monday - Friday	7:30 am - 5:00 pm

McKenzie Building Hours*

Monday - Thursday	7:30 am - 11:30 pm
Friday	7:30 am - 7:30 pm
Saturday	9 am - 9:30 pm
Sunday	9 am - 8:30 pm

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

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