University of Oregon

COMPUTING NEWS

Summer 2005

The Willamette River runs northward through the heart of the Willamette Valley and provides a major source of natural and recreational resources to the most densely populated region of Oregon.

IN THIS ISSUE…

Microcomputing

UO Large Systems

UO Libraries Update

Administrative Computing

Telecom

Security

Statistics

People

Interesting Sites

UO Moves to McAfee for Antivirus

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

Although the University of Oregon has traditionally site-licensed the retail edition of Symantec Norton Antivirus (NAV), it is switching to McAfee's antivirus product for the 2005-6 academic year.

Why Change?

Previously, the UO had a somewhat unusual relationship with Symantec. According to Symantec, the UO was the only school in the world with a site license for the retail version of NAV. This year Symantec indicated that it wanted to cease supporting site-licensed use of that product and was unwilling to continue offering it to us.

UNIVERSITY OF OREGON

COMPUTING CENTER

COMPUTING NEWS
VOL. 20 #3

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

Contact: Joyce Winslow
jwins@uoregon.edu

Photography: Dave Ragsdale
dave@uoregon.edu

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

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

Got Extras?

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

This meant that, quite aside from any other considerations, it was appropriate to look at other antivirus products.

While we could have moved from the retail edition to the corporate edition of Symantec, the corporate edition was a poor fit for the UO's decentralized PC environment.

In addition, Symantec had changed its pricing structure to encourage customers to purchase a security product bundle instead of Norton Antivirus alone. This would have made moving to the corporate edition considerably more expensive.

Reviewing Our Options

Given these circumstances, we took the opportunity to review our antivirus alternatives. Naturally our first objective was to determine which antivirus product did the best job of detecting and removing viruses.

Putting products to the test. To address that question, we obtained a customer's permission to use his virus-infected system as a test case and made a reference copy of his system. We then tested different antivirus products on the infected system. After testing one product, we returned the laptop to its original infected state and tried the next product.

It was not unusual for antivirus products to find viruses that they couldn't remove—with one noteworthy exception: McAfee. McAfee was able to remove *every* virus it found.

Researching peer universities: When making a decision such as this, it is sometimes helpful to see what other schools are doing. With that in mind, we looked at antivirus-related web pages for other Internet2 member universities. Of the 177 schools that had published information on their antivirus product choice at the time of our study, just over 50% used Norton and just under 40% used McAfee. All other antivirus vendors' products were employed at half a dozen sites or less.

Other considerations. We also looked at things such as ease of use, product speed, support options, how well the product integrated with the operating system and applications, how virus definition updates were handled, and a range of other factors.

After taking all this into account, we concluded that McAfee would be the best solution for the university for the 2005-6 academic year. In moving to McAfee, we join a list of other McAfee university customers that includes Arizona State, Chicago, Florida State, Georgia Tech, Hawaii, Harvard, Idaho State, Illinois Urbana-Champaign, Kentucky, Massachusetts, Michigan, MIT, Montana State, Nebraska, New Hampshire, New Mexico State, North Dakota, Notre Dame, Ohio State, Oklahoma State, Rutgers, South Carolina, Texas, Utah State, Wisconsin-Milwaukee, Utah, and Washington.

What Did We License?

For UO students: Student Windows PC users will be using McAfee Virus Scan (PC) under the Student Use Option, along with McAfee Anti-Spyware (PC) under the Student Use Option. Student Mac Users will be using McAfee Virex under the Student Use Option.

For faculty and staff: UO faculty and staff will be using McAfee Active Virus Scan Suite PerpetualPlus License, plus McAfee Anti-Spyware PerpetualPlus for Windows or

McAfee Virex PerpetualPlus for the Mac, including the home use option for these products.

How Do I Get McAfee?

If your department centrally manages all of its desktop computers, your department's technical support staff will likely already have access to McAfee—and in fact you may already be running it. (Departmental staff who still need to arrange access to McAfee software for managed desktop installation should contact Microcomputer Services, **346-4412**.)

CD copies of the Windows McAfee products for individual installation should be available for UO faculty, UO students, and UO staff at normal Duckware distribution locations* by mid-July. To get a copy of McAfee you will need to show a current UO ID card.

We are also working on an online download option that requires logging in using your UO user ID. Check **http://micro.uoregon.edu/av/** for more information about the status of that alternative.

CD copies of Virex for the Mac will be available shortly, upon conclusion of McAfee's final beta testing of a Tiger-compatible version.

Questions

Q I don't want to change to McAfee! Can I stay with Norton?

A The University's license for Norton expires July 27th, and we will not be supporting that product beyond that time. McAfee is the product we now have licensed as a replacement. We strongly urge you to give McAfee a chance. We think you'll really like it.

That said, you do always have the option of individually licensing an alternative product. (Central funding and support will not be available for antivirus products other than McAfee, however.)

Q Can I share my copy of McAfee software with a few friends?

A No. McAfee, like all commercial antivirus software, is a copyrighted product. The university has purchased a fixed number of licenses for McAfee and is carefully tracking usage to ensure that we stay within our licensed limits. We need your cooperation to make sure that we do so—and that includes *not* making McAfee available to anyone other than UO faculty, UO students, and UO staff.

***Distribution locations:**

- Microcomputer Support Center (151 McKenzie Hall)
- Documents Room Library (175 McKenzie Hall)
- CC-McKenzie Lab (101 McKenzie Hall)
- CC-EMU Microcomputing Lab (22 EMU)
- CC-Klamath Lab (B13 Klamath Hall)
- CC-Millrace Lab (113 Millrace I)
- AAA (280 Lawrence Hall)
- Knight Library Information Technology Center (second floor, Knight Library)
- Science Library Information Technology Center (lower level, Onyx Bridge Building)

All New Student Accounts Now Being Created on Darkwing

If you've been at the University of Oregon for some time, you are probably aware that most undergraduate students have traditionally been issued accounts on Gladstone, while most faculty, staff and graduate students have been issued Darkwing accounts.

As part of the process of upgrading and simplifying our large shared systems, and because Darkwing will be far more scalable than the old Gladstone, new undergraduate accounts are being created on Darkwing this year instead of on Gladstone. Faculty, staff and graduate accounts will also continue to be created on Darkwing as has traditionally been the case.

We are alerting you to this change here so that if you work with new students you are not confused or surprised to learn that new undergraduate accounts are being created on Darkwing rather than Gladstone.

What About Existing Gladstone Users?

Existing Gladstone accounts will also be merged onto Darkwing, but before we can do that we need to contact and work with a few hundred users who have both Gladstone and Darkwing accounts to ensure that their accounts can be cleanly combined.

If you are one of those comparatively rare users with both a Gladstone and a Darkwing account, expect to be contacted by Computing Center staff with further details about what we need you to do in the months ahead. All other Gladstone users need do nothing at this time.

What About Existing Darkwing Users?

Existing Darkwing users need do nothing at this time.

Telecom Services Offers Discounted Wireless Phone Service to UO Employees

UO departments may choose from an expanding array of wireless service options for conducting state business

Lori Hansell
Customer Service Administrative Assistant, Telecom Services
lhansell@uoregon.edu

Did you know that cellular phone service for University of Oregon (state) business use is available at very reasonable prices to UO faculty and staff? You can order this discounted service through UO Telecom.

UO Telecom currently supports wireless service through two of the most popular carriers, Verizon Wireless and Cingular. Both companies offer BlackBerry, Treo, and smartphones, and for an additional fee you can add text messaging, picture messaging, and paging. Package pricing for these messaging services is also available. You'll find wireless service order forms on Telecom's website at **http://telcom.uoregon.edu/cellular.htm**

Comparison Shopping

Which service should you choose? Here's a brief summary of the differences between Cingular and Verizon services to help you make your decision:

Cingular. If you travel abroad, Cingular, which has a significant international footprint, is worth considering (note that a quad-band or higher device is recommended). Cingular offers the best coverage for data services, and its voice coverage is improving on a daily basis.

Verizon. Verizon offers a wider range of voice coverage and its rate plan prices are a bit more competitive. It also charges considerably less for data equipment. We are currently working to provide Verizon users with even larger discounts.

Verizon transfers data faster than Cingular but has a limited coverage area. With a slight modification, its phones will work in South Korea.

General note: Pricing on rate plans and equipment differs from what is offered to the general public, and equipment prices change monthly—even weekly—and cannot be guaranteed.

By ordering through Telecom, you're assured of excellent customer service, warranty support, discounted or waived fees, and the flexibility to modify your plans and equipment during the service period without penalties. As an added convenience, your cellular phone charges will appear monthly on UO departmental phone bills. Rental phones are also available through Telecom for local or international use.

Also note that these particular wireless service discounts and benefits are offered *only* through Telecom, and that Telecom does not support accounts set up by individuals.

If you have any further questions regarding pagers, cell phones, wireless plans, or policy, please contact Lori Hansell (*lhansell@uoregon.edu*, **346-1035**).

Apple Recalls Laptop Batteries for some G4 Models

Citing a potential fire hazard, Apple has issued a voluntary recall of approximately 128,000 rechargeable laptop batteries for its 12-inch iBook G4, 12-inch PowerBook G4, and 15-inch PowerBook G4 models sold from October 2004 through May 2005. The recalled batteries' model numbers are shown in the chart below. Affected batteries have *both* a model number *and* a serial number from those batches, so check both.

Computer Model	Battery Model #	Battery Serial # Range
12-inch iBook G4	A1061	HQ441 - HQ507
12-inch PowerBook G4	A1079	3X446 - 3X510
15-inch PowerBook G4	A1078	3X446 - 3X509

Customers are advised to stop using the recalled batteries immediately and contact Apple to arrange for a free replacement. For more details on how to check your batteries and return them if necessary, see Apple's support page at **http://www.apple.com/support/batteryexchange/** For more information about the hazards of these defective batteries, see the U.S. Consumer Product Safety Commission report at **http://www.cpsc.gov/cpscpub/prerel/prhtml05/05179.html**

Don Harris is the UO's New Vice Provost for Information Services and Chief Information Officer

New IT chief to take charge in August

Concluding a search that began after Joanne Hugi's retirement in 2004, the University of Oregon has selected Don Harris to head its information technology services.

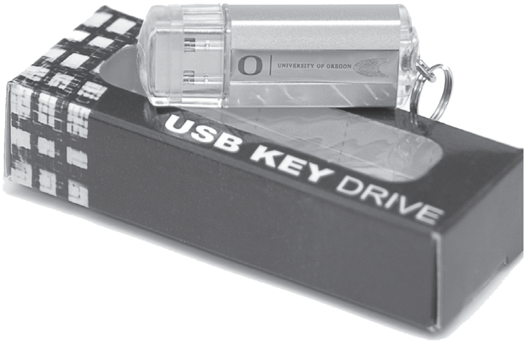
Harris holds a doctorate from the Claremont Graduate University, and bachelor's and master's degrees from Biola University. He has been vice provost for information technology and chief information officer at Emory University since 2001, and he will hold the same title at the UO.

Prior to his appointment at Emory, Harris served as associate vice president for information systems at the University of Memphis. He has also held academic and administrative positions at Messiah College, the University of Maryland, and Pepperdine University.

He will begin his new job in early August, reporting to John Moseley, senior vice president and provost.

New USB Thumb Drives Show School Spirit

The E-Shop is stocking new metal thumb drives sporting UO logo



If you're looking for a portable backup solution, you may be interested to learn that the Computing Center's Electronics Shop in 151 McKenzie Hall has a new line of durable metal USB Flash Drives emblazoned with the UO's trademark **O**

These handy metal drives are small enough to fit in your pocket and can be plugged into any USB port. No power supply or cables are needed. Despite their toy-like appearance, the drives have a lifetime of up to one million rewrites and can retain data for up to 10 years.

The nonprofit E-Shop stocks USB thumb drives in a variety of sizes: 32MB ($15), 64MB ($20), 128MB ($25), 256MB ($35), 512MB ($60), and 1GB ($100). In addition, the shop sells 1GB *bootable* USB Flash Drives for $120 each.

Wireless Cards. You'll also want to visit the E-Shop if you're in the market for D-Link wireless cards for your laptop or desktop computer. These cards are competitively priced, and you can get help with installation and set-up on the spot at no charge.

The E-Shop is located on the ground floor of McKenzie Hall in Room 151. It is open weekdays from 8 A.M.to 5 P.M.

For more information about E-Shop services, call **346-3548**, email *hardwarehelp@uoregon.edu,* or visit **http://cc.uoregon.edu/e_shop.html**

Who's Who at the Computing Center

Meet our new EMU Computer Lab manager…

Joyce Winslow
jwins@uoregon.edu

Sam Crow, EMU Computer Lab Manager

After nearly four years as a student lab consultant in the EMU Computer Lab, Sam Crow stepped into his new role as the lab's manager as easily as if it were an old pair of slippers. His deep technical background, inquiring mind, and helpful nature make this third-generation Oregonian a natural for the job.

Sam's electronic know-how was recognized early in life, and he was always the neighborhood go-to guy for computer problems in Madras, the small Central Oregon ranching community where he grew up. After high school, he gained more advanced technical experience in the Navy, where he was a sonar operator on a ballistic missile submarine.

Always seeking new experiences and a wider world, Sam's next move after his tour of duty was to enroll at the University of Oregon in the fall of 2001. He chose a course of study that mirrors his diverse interests, majoring in English with a minor in Computer Information Technology.

Sam's stint with the EMU Computer Lab began in September 2000, when he was hired as a student lab consultant. Sam found himself in his element: solving problems, helping people, providing a valuable service. He considers his current job as manager, which he assumed last March, a vital hands-on learning experience that will round out his education in his chosen field of educational technology.

Sam often refers to himself as a "dreamer," but if that were true, he couldn't possibly meet the many pressing demands being made upon him. As lab manager, he's now responsible for the "big picture": not only assisting users, but overseeing staff, participating in policy decisions, installing and maintaining new management software for security and imaging, troubleshooting hardware and software problems, and ensuring that day-to-day operations run smoothly.

Outside of work, Sam's independent streak is manifest in his unorthodox mix of enthusiasms. He prefers Marlowe to Shakespeare, and is equally at home with Mozart and Metallica. He's a devotee of both science fiction *and* 16th century English literature. And while undeniably a bit of a bookworm, capable of scribbling reflectively for hours in his journal while his cat, Penelope, snoozes nearby, Sam is most definitely not a couch potato. His favorite form of recreation is hitting the road on his prized motorcycle, a Kawasaki Vulcan 750. This summer he plans to take his bike on some longer rides to Crater Lake, the coast, and Central Oregon.

Campus Surplus Website:

Does your UO department have office furniture, computer equipment, or software it no longer needs? Are you looking for another filing cabinet or an extra CD or DVD drive?

Whether you want to recycle excess equipment or find something that meets your needs, the Department Surplus Listings website at **http://surplus.uoregon.edu/** is for you. This clearly organized website allows you to sign up for email notification when an item of interest is posted, list your own department's surplus items (with photos if desired), and browse current listings by category. Take a moment to check out the surplus website today. It's a great opportunity to share the wealth!

Summer and Fall Blackboard Upgrades Scheduled

As the Blackboard system matures, you can expect some significant changes; we've scheduled system downtimes to minimize inconvenience

JQ Johnson
Director, Center for Educational Technologies
jqj@uoregon.edu

In 2005, the number of UO courses using the Blackboard system grew by about 40% over last year, and we're anticipating continued growth next year. The system is also maturing, with new releases from the vendor and new features.

To allow time for upgrades, the UO Libraries have developed a new schedule for Blackboard system downtime for the next year. The schedule aligns Blackboard's downtime with Banner's, providing adequate downtime for necessary system upgrades but avoiding downtime and upgrades during periods that will seriously impact our Blackboard user community.

Our plan is to reserve the morning of one Saturday every month—typically the second Saturday of the month—for system downtime. This schedule is almost identical with the Computing Center's schedule for Banner maintenance. Such Saturday downtime periods will not be taken every month, and they will be limited to 6 A.M. to 1 P.M. Except in emergency situations, at least one month of advance notice will be given for all scheduled downtime.

In addition, the system will continue to be down every Monday morning from 6 A.M. until 8 A.M. for data backup and minor system upgrades, and will be down briefly (for approximately two minutes) every day at about 4 A.M. The downtime and upgrade schedule for the rest of 2005 includes:

Date	Planned Downtime Schedule
July 9, 2005	RedHat AS 3.0; additional minor upgrades
Aug 13. 2005	major version upgrade: Blackboard 6.3
Sept 10, 2005	additional 6.3 updates
October 8, 2005	tentative: 6.3 service pack 1
Nov 12, 2005	tentatively scheduled; no major user-visible changes
Dec 17, 2005 (third Saturday)	tentative: upgrade to Blackboard 7.0

The most significant upgrades currently planned are at the end of summer, when we upgrade to Blackboard 6.3 (also known as "Application Pack 3") and during winter vacation, when we upgrade to version 7.

Blackboard 6.3 is a major upgrade, the most substantial we've had since 2003. Significant new features include:

- **Advanced Assessment questions:** a completely revamped online quiz implementation featuring several new types of questions, such as "calculated formula," "file upload," "hotspot," "Likert scale," and more.
- **Adaptive Release:** allows the instructor to control on an individual-student basis what portions of a site are available, for example based on prior quiz performance.
- **Multilingual Support:** locales that allow system messages and menus in languages other than English.
- **Performance Dashboard**
- **Review Status**
- **Assessment Question Completion Status**
- **Syllabus Builder**
- **SCORM 2004 (Sharable Content Object Reference Model):** aids content developers in producing content that is sharable, reuseable, and interoperable.
- **Advance Navigation Bar**
- **Gradebook Null Option**

Documentation for 6.3 is expected to be available in early July from the Blackboard support website at **http://behind.blackboard.com/**

Meanwhile, faculty interested in taking advantage of the new features of Blackboard 6.3 can go to **http://libweb.uoregon.edu/cet/blackboard/news/** or contact JQ Johnson at *jqj@uoregon.edu* for more information.

MATHEMATICA 5.1.1 UPDATE AVAILABLE

Wolfram has provided the UO with an update to Mathematica. For more information on installing Mathematica on university-owned computers, see **http://darkwing.uoregon.edu/~hak/mathematica/** Please note that home use is limited to faculty only. Email Hans Kuhn at *hak@uoregon.edu* for details.

Tiger, Tiger, Burning Bright…

Apple's latest operating system boasts a number of stellar enhancements

Patrick Chinn
Distributed Network Computing Consultant
pchinn@uoregon.edu

Small details are what turn a house into a home, and this is also true of operating systems. After all, some of us spend eight hours (or more) a day working and playing in that digital space!

Apple's April release of Tiger, also known as Mac OS X 10.4, introduced a few new big features (Spotlight and Dashboard) and several hundred small features. While Spotlight and Dashboard have been the focus of most of the publicity, many of the small changes help make Mac OS X 10.4 an easier and more comfortable place to work and play.

Spotlight. Spotlight is Apple's new search technology. Most search utilities look for a file using the name you specify, a strategy often doomed to failure because a file's name may not directly match the file's content. Apple had previously attempted to solve this problem by offering file content searches, where the contents of your files are searched along with the file names. Those efforts failed because the process was too slow.

Spotlight attempts to solve this problem by using a new technique: every time a file is opened or saved to your computer the contents are added to the master index, producing a constantly updated and (relatively) fast way to search your computer. A Spotlight search for a single word will return text files, Word and Excel documents, PDFs, photos, email messages, music, calendar events, fonts, and nearly every other type of file on your computer.

However, Spotlight is not without some limitations. Primarily, some files, like Microsoft Entourage email databases, cannot be searched until the program is redesigned by its publisher. Secondly, Spotlight cannot index all file types automatically; some files require a Spotlight plug-in. Lastly, performing a file content search is excessive when you know the file name and need only that simple search.

Spotlight has already spawned its own new feature: smart folders. By creating a new smart folder (select "New Smart Folder" from the File menu in the Finder) and entering search criteria, the folder will automatically display those items that match your search terms. Create a smart folder that displays files larger than 100MB to help you find and remove big, space-wasting files on your computer. Or, if you often name files based on projects, create a smart folder that lists all files by project.

Dashboard. Tiger's new Dashboard has also garnered some press. Dashboard is a synthesis of desk accessories from Mac's days of old and Exposé, the window-shuffling feature added in Mac OS X 10.3. It provides extra desktop space reserved specifically for utilities called "widgets." Invoke Dashboard by pressing F12, and the Dashboard zooms into place, revealing the default set of widgets: a calculator, a clock, a calendar, and the current weather. Press F12 again to make the Dashboard disappear.

Apple includes translation, dictionary, address book, iTunes, and stock price widgets, among others. Many other widgets have been created since Tiger's release. See **http://www.apple.com/downloads/dashboard/** for several hundred more widgets.

Mail updates. Mac OS X 10.4 has redesigned Mail's main window, removing the pop-out list of mail folders and integrating it into the main Mail window. The way Mail handles pictures has also been improved. For outgoing messages with photos, Mail provides on-the-fly picture resizing in four sizes (small, medium, large, and actual size). It also indicates the size of the outgoing message, making it much easier to ensure your messages are under the 5MB email attachment limit. Look for these two features at the bottom of the new message window after you've added pictures to the message.

Another new feature is that Mail offers an iPhoto-like slideshow when a mail correspondent sends a set of pictures via email. Look for the Slideshow button next to the Save button below the subject line of the message. Slideshow lets you move backward and forward through the pictures, view a contact sheet of all photos, zoom the image to fill the screen, and, in some cases, add the image to iPhoto.

This same slideshow feature also made its way into the Finder. Select a group of pictures, command-click on one of them, and select "Slideshow" from the menu that appears. This feature has limits: it will not traverse folders within your selection to display photos, which means you can't watch a slideshow of photos that are organized into folders.

Spell checking-plus. Earlier versions of Mac OS X provide system-wide spell checking. Tiger supplements this feature with the addition of the New Oxford American Dictionary and the Oxford American Writer's Thesaurus. To look up a word, highlight and command-click it and select "Look up in Dictionary" from the contextual menu. The dictionary also runs as an application; you can find it in the Applications folder.

Safari enhancements. Apple's web browser Safari also received some attention from Apple's programmers in the form of private browsing, RSS support, PDF viewing, and emailing web pages.

The most talked-about new feature is RSS support. RSS (Real Simple Syndication) is a headline-and-summary version of web pages that some websites offer as supplements to their full-featured pages. When Safari loads a web page with RSS, it displays a blue "RSS" button in the address bar. Click the blue button to view the RSS version of the page. Since RSS addresses are stored like any other bookmark, you can create a folder that contains similarly themed website feeds. Set that folder to open all links when clicked by checking the "Auto-Click" box in the bookmark management window. When you click that folder button, Safari will then load all the feeds on one page.

In Safari's new Private Browsing mode, the program does not cache web pages, make history entries, or track text entered in the search field, among other things. This feature effectively obscures a person's web-browsing habits, a wise choice for those who use Safari on publicly-accessible computers.

Another new feature is Safari's ability to mail a web page address, or the page itself, directly from within the application. When you select "Mail Link to This Page" from the File menu, Safari automatically creates a new mail message (in Mail) with the web page's address listed in the body of the message. The "Mail Contents of This Page" command will create a new mail message (again in Mail) and insert the current web page into the body of the message.

Safari also now displays PDFs in a browser window without requiring a plug-in. Given the ubiquity of PDFs, this feature is a welcome addition. Simply click on a link to PDF and the application will display the file in a browser window. This feature lacks some of the advanced options that other PDF plug-ins provide, but it offers the basic functions of zoom in and out, auto-size document to the window, and view with Preview (Apple's image viewing application).

Troubleshooting help. Apple has added a few features to help troubleshoot web browser and email connection problems. Tiger's version of Safari will present you with a "Network Diagnostics" button if the program cannot connect to the Internet. In my tests, Network Diagnostics did a good job of using plain English to step me through the troubleshooting process. Mac OS X Mail's Connection Doctor will test whether the mail program can connect to each of the mail servers configured in the program. Connection Doctor was more useful to me as a connection summary than as a troubleshooting tool, especially compared to Network Diagnostics.

Augmented parental controls. In prior versions of Mac OS X one could limit a user's access to specific applications. With Tiger, parents can create a list of allowable websites, email addresses, and Internet chat participants for each account on the computer.

Address Book additions. In Tiger, Address Book has become a more mature application. With a few clicks you can print an envelope with the selected person's address, and you can also print a pocket address book from the data stored in Address Book. Apple has also added more import options, making it easier to move your data into Address Book.

CD-burning extras. To augment the Finder's CD-burning feature Apple added burn folders to Mac OS X 10.4. Create a burn folder by selecting "New Burn Folder" from the File menu, drop the files you wish to write to CD into that folder and then click the burn button in the top right corner of the window. This new feature is especially handy if you have a collection of files or folders that you frequently burn to CD (for backup purposes, for example).

And more… Mac OS X 10.4 has many other new features not covered here. For more information on all the new features in Mac OS X 10.4, see

http://www.apple.com/macosx/

UO site license. The UO has purchased a site license for Mac OS X, which makes Tiger free to current UO students, faculty, and staff. You may borrow an installation DVD or CD-ROM set from the Documents Room (175 McKenzie Hall) or buy an installation DVD from the UO Bookstore's Digital Duck (895 E. 13th Avenue). For more information about the UO site license for Mac OS X, see

http://micro.uoregon.edu/macosx/licensing/

A Note on Tiger Incompatibilities…

Before upgrading to Tiger, you should check to make sure that your existing software applications and utilities are compatible.

Microcomputer Services is maintaining a website that tracks Mac OS 10.4's compatibility problems with software that's commonly used at the University of Oregon (see **http://micro.uoregon.edu/macosx/tiger/**)

For a complete list of Tiger's known software compatibility issues, see Macintouch's "Tiger Review: Incompatibilities and Workaraounds" at **http://www.macintouch.com/tigerreview/incompatibility.html**

Information on Hard Drives in Surplus Hardware:

Before recycling, make sure your discarded computer system is completely purged of sensitive information

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

When desktops or laptops are replaced or become obsolete, they are commonly transferred to another department or disposed of as surplus property.

Before transferring or disposing of any UO computer system, it's important to make sure any sensitive data formerly stored on the system has been *completely* removed.

While university data is not as highly classified as that of the Department of Defense (DoD) or law enforcement and intelligence agencies, the UO does work with confidential administrative and academic data. These data include student records, human subjects-related academic research data, health-related information, financial data, passwords, and the like—all of which must be protected from unauthorized disclosure in compliance with the requirements of FERPA, HIPAA, GLB, Sarbanes-Oxley, and other applicable state and federal privacy regulations.

The Problem: "Delete" or "Format" is NOT Enough

Non-technical users may assume that simply "deleting" the files on a system's hard drive (or "formatting" that disk) may be sufficient to destroy the contents of that drive or disk.

Unfortunately, that is not the case: simply "deleting" files or "formatting" a hard drive will *not* be enough to definitively destroy information formerly stored on that drive. In fact, deleted files or information on a formatted drive will most likely still be recoverable—which means that private or sensitive data is vulnerable to inappropriate disclosure if special additional measures aren't taken.

For example, a recent article (see "Dumped hard drives tell all" in the References section below) reported that 113 of 200 drives purchased on eBay as part of a security vendor's study on disk sanitization still contained recoverable data, including data that in some cases appeared to be confidential or quite personal in nature. If you are transferring or surplusing a university computer system, you *must* sanitize that machine before transferring or otherwise disposing of that system.

How to Sanitize a Disk

There are two common approaches to sanitizing disks in a system. The first is to employ a software disk "wiping" or "overwriting" utility. The other is to physically destroy the hard disk by incinerating, melting, crushing, or shredding it.

Disk Wiping. If you'd like to employ a disk wiping utility to successively overwrite a surplus hard drive with various specified or random patterns, look for a disk wiping utility that at least meets the DoD 5220.22-M standard (not all disk wiping utilities do; it is common for some commercial products to offer a less thorough wiping mode as part of a free "trial," only providing a DoD 5220.22-M-compliant version upon payment of an additional fee).

Examples of commercial and open source products which perform software disk wiping include (in alphabetical order):

- CyberScrub's cyberCide
  http://www.cyberscrub.com/ (~$36)
- DBAN: Darik's Boot and Nuke
  http://dban.sourceforge.net/ (free)
- Eraser
  http://www.heidi.ie/eraser/ (free)
- WhiteCanyon's WipeDrive
  http://www.whitecanyon.com/
  (~$40)

Although wiping a drive to DoD 5220.22-M standards will normally be sufficient, it is not foolproof.

For example, software disk-wiping utilities obviously cannot sanitize disconnected and forgotten internal hard drives, or hard drives that have physically failed. Likewise, disk wiping is not government-approved for sanitizing particularly sensitive information (such as Department of Defense top secret information) because of the possibility that a particularly determined adversary might be able to recover inter-track residual data.

In other cases, using a software disk wiping tool may take far too much time, particularly if you have lots of drives or extra-large drives (remember that disk wiping tools repeatedly overwrite the entire drive, a process that can take minutes to hours depending on the number of passes performed, the size of the drive, and the speed of the system).

Hard Drive Destruction. When DoD 5220.22-M standard software disk wiping isn't enough, drives will normally be removed from the host computer and then destroyed by melting, incineration, crushing, or shredding.

Obviously the physical removal of a system's hard drive(s) this way takes time, and renders the remainder of the system unusable without a replacement disk. This may result in some dead-on-arrival systems being demanufactured (or junked outright) rather than being reused, a point that can rightfully cause concern in these times of tight budgets and overflowing landfills.

'Deleted' Does Not Mean 'Gone'

On the other hand, the potential costs associated with compromised data can be huge, and aging computer hard drives, perhaps more than any other system component, are prone to catastrophic physical failure and a resulting loss of data. Considering those factors, investing in a comparatively inexpensive newly manufactured replacement drive may prove to be a real bargain in the long run!

Let me also stress that we do *not* recommend that you attempt to physically destroy surplus sensitive hard drives yourself. Most individuals and departments do not have suitable facilities to do this safely and in an ecologically sound way, and it is easier to fail at irrevocably destroying a hard drive than you might think. For example, see the March 2004 *Network World* article "Inside the DoD's crime lab," which recounts how the Department of Defense computer forensics lab has been able to successfully recover hard drives that have been "thrown off of balconies and even shot with AK-47s, as in one recent battlefield case."

If you do need to physically destroy hard drives that contain sensitive information, many of the same companies that offer certified secure document disposal also offer certified secure hard drive destruction services.

A Brief Check List of Some Additional Precautions

1. **Obsolete systems may not be the only systems needing sanitization.** For example, leased systems may also contain sensitive information when they're returned to the leasing company.
2. **The hard drive may *not* be the only storage media in a system.** Beware of floppy disks left in floppy disk drives, Zip disks in Zip drives, CDs and DVDs in optical drives, tapes in tape backup units, thumb drives/compact flash drives, BIOS passwords, and the like.
3. **Include relevant documentation before transferring a system.** When licensing permits, particularly when an old system is wiped and then transferred from one university department to another, it is helpful if the original operating system license, media, and documentation are included with the surplus system at the time it is transferred.
4. **Desktops and laptops aren't the only systems that need sanitizing**. PocketPCs, PDAs, some multifunction cell phones, and other devices may also contain sensitive information such as passwords or confidential data.

If you're a UO user with questions, comments, or feedback about this article, feel free to email me, Joe St Sauver, at *joe@uoregon.edu*

References

1. "Dumped hard drives tell all," May 31, 2005 **http://news.com.com/2061-10789_3-5726835.html**
2. "Inside the DoD's crime lab," *Network World*, March 2004, **http://www.networkworld.com/research/2004/0308dod.html**
3. "National Industry Security Program: Operating Manual (DoD 5220.22-M)," **http://www.dss.mil/isec/nispom.htm**
4. "Remembrance of Data Passed: A Study of Disk Sanitization Practices," Simson L. Garfinkel and Abhi Shelat, *IEEE Security & Privacy*, Jan/Feb 2003, pp. 17-27. **http://csdl.computer.org/dl/mags/sp/2003/01/j1017.htm**

Industry News

Apple Opts for Intel

At its Worldwide Developer Conference on June 6, Apple confirmed the rumor that its future Macintosh products would contain Intel microprocessors. To smooth the transition, Apple is providing a Developer Transition Kit to software developers. Microsoft Office for Mac and Adobe software makers have already announced plans to adapt their software accordingly.

http://www.macintouch.com/
http://www4.macnn.com/macnn/wwdc/05/

Next Version of Microsoft Office will Include XML

Extensible markup language (XML) will become standard in Microsoft Office next year, according to company officials. The new Microsoft Office, code-named "Office-12," will employ default XML formats for Word, Excel, and PowerPoint.

http://www.theregister.co.uk/2005/06/03/_office_xml/

Trend Micro Acquires Kelkea

In a move calculated to strengthen and expand its line of antivirus and Internet security software solutions, Trend Micro announced its acquisition of Kelkea on June 14. Over the past eight years, Kelkea, which is known for its anti-spam and anti-malware technologies, has assembled a valuable knowledgebase of statistics and history for more than 1.5 billion IP addresses.

http://www.trendmicro.com/en/about/news/pr/archive/2005/pr061405.htm

House Bill Attempts to Curb Government-Owned Telecom

In June, U.S. Rep. Pete Sessions (R-Texas) introduced a bill to prohibit state and local governments from offering telecommunications services in any area already covered by a private entity.

http://www.internetnews.com/wireless/article.php/3509961

To Upgrade or Not to Upgrade, That Is the Question…

When's the best time to upgrade to the latest and greatest?

Chris Jones
Director of Computing Services, School of Architecture & Allied Arts
jonesey@uoregon.edu

Computer owners are often faced with a choice: should I upgrade my operating system or other software, or should I stick with what I have for now?

In the Spring 2002 edition of *Computing News* (**http://cc.uoregon.edu/cnews/spring2002/osx.html**), Patrick Chinn wrote an article entitled "Should You Upgrade to Mac OS X?" It contained a bit of useful advice that I don't hear very often, and I'd like to expand on it in this article. His good advice was: "We recommend using your current operating system until it's time to upgrade to a new computer."

Patrick's advice will seem radical to people who believe that it is important to have the latest and greatest software on the market. They grasp at every shiny plaything that software makers dangle in front of them, often to their detriment. There are a few good reasons to upgrade software and many good reasons to wait. There are exceptions to every rule, of course, but in ten years of helping people with computers, I have found these rules to be true almost all of the time.

Here are a few reasons to avoid upgrading your operating system or application software on a computer you currently own:

1. **New software will slow down your computer**
   Almost every software upgrade demands more memory and more of your computer's processing power. The visible symptom of these demands is sluggishness. Your computer will be slow to perform your usual tasks. If you avoid upgrading software, your computer will perform faster, and you should experience less frustration.
2. **Avoid the "upgrade cascade"**
   After you shell out money to upgrade your software, you often discover that you need more memory and upgrades to other programs that are incompatible with the software you upgraded. The computer's newfound slowness will start you thinking about a new computer sooner than you otherwise would have. Major operating system upgrades (e.g. Windows 98 to XP, or Mac OS 9 to OS X) are especially susceptible to the upgrade cascade, often causing computer owners to have to upgrade many pieces of software or download new drivers for peripherals.
3. **New software is often buggy**
   I strongly urge my customers to wait a few months after a new operating system or program comes out before they take the plunge and upgrade. Current software development techniques are such that software is typically released before all of the bugs have been squashed. Within the first few months after a program's release, the software maker usually releases "service packs" or "patches" that fix bugs and improve performance. Let other people test new software while you maintain your productivity.
4. **It is easiest to make a transition all at once**
   If you wait to upgrade your operating system and software until you get a new computer, you have to make just one transition every three or four years, rather than a series of time-consuming transitions, one or more each year. A computer is just a tool for most of us; the less time we spend fiddling with it, the more time we have to do the work that the university asks us to do.
5. **Software costs money**
   This may seem obvious, but you can save money by staying off the upgrade treadmill. By waiting to upgrade until you get a new computer, you can often skip a version or two of the software you use, saving time and money in the process.

Here are a couple of times when it is *right* to upgrade:

1. **Sometimes you can't do your job without an upgrade**
   If your co-workers or colleagues are sending you work-related documents that you are unable to open, you may need an upgrade. Sometimes, you can ask your colleagues to save their documents in a compatible format, but if this works at all, it will work only for a while. Likewise, administrative units on campus may require the use of certain programs or versions of programs in order to interact with the UO's administrative systems. If this is the case, you'll need to upgrade in order to continue doing your job.
2. **Your current operating system is no longer supported**
   Computer operating system makers typically discontinue support for operating systems after they have been on the market for about six or seven years. If you bought a computer three years ago with a three-year-old operating system on it, your operating system was probably fully mature and quite stable, but it may soon lose support. If you plan to hold on to the computer for another two or three years, an operating system upgrade (along with a memory upgrade) is probably a good idea.

« cybercrime in the news »

419 Scams Keep Evolving

419 email scams, once easily identifiable by their quaintly worded pleas for help in recovering large sums of money trapped in overseas banks, are no longer so easy to spot. Taking cues from the headlines, these scams have morphed to exploit people's sympathy for tsunami victims, Iraqis wronged by Saddam Hussein, and even the families of American soldiers killed in Iraq.

There are still other nefarious variations on these scams that employ chat rooms for singles, exploit the Internet Relay system for the deaf, buy merchandise on online auction sites with bogus cashiers checks, and even create fake banks on the Internet.

The common theme in all of these scams is conning a victim into sending money via wire transfer overseas. To learn more, see the report at
http://www.msnbc.msn.com/id/8171053

British Hacker Arrested for Breaking into NASA, Pentagon Computer Systems

Gary McKinnon, an unemployed former computer engineer described as "the world's biggest computer hacker," was arrested in June and charged with breaking into vulnerable computers in US military networks and hacking the networks of six private companies and organizations. For details, see
http://www.thisislondon.co.uk/news/articles/19164714

MSN Site Hacked in South Korea

In June, hackers booby-trapped the MSN website in South Korea in an attempt to steal passwords from visitors. The break-in was thought to be facilitated by the site administrators' failure to apply Microsoft software patches. For details, see
http://www.crn.com/sections/breakingnews/ breakingnews.jhtml?articleId=164300062

C3 Targets Internet Crime

Child exploitation via the Internet is being aggressively investigated by a state-of-the art forensic computer lab known as the Cyber Crimes Center (C3). C3, which is part of the Department of Homeland Security, is run by the U.S. Immigration and Customs Enforcement agency. In addition to combating child porn, C3 has also gone after a global network of software pirates and has helped identify Internet rug dealers. For details, see
http://www.pittsburghlive.com/x/tribune-review/trib/ mostread/s_340904.html

UK Bans Internet Porn Sales

A British high court has upheld a ban on sending videos or DVDs through the mail or selling them online. For details, see
http://www.theregister.co.uk/2005/05/24/ adultshops_no_mailorder/

Hackers Turn to Extortion

Some hackers are now engaging in extortion plots. Employing a new form of attack known as "ransom-ware," they hack into a victim's system, lock up valuable data, and demand a ransom for releasing it. For details, see
http://www.wired.com/news/business/0,1367,67622,00.html

Florida Man Pays Hefty Fine for Illegal Spamming, Making False Product Claims

After paying nearly $500,000 in consumer redress, Creaghan A. Harry is barred from making any further claims about "anti-aging"/ "HGH" products sold over the Internet. Harry, who does business as Hitech Marketing, Scientific Life Nutrition, and Rejuvenation Health Corporation, reached a settlement with the Federal Trade Commission nearly one year after being charged with violating the FTC act and anti-spam laws. He may yet face costs of $5.9 million. For details, see
http://www.ftc.gov/os/caselist/0423085/0423085.htm

GAO Finds DHS Cybersecurity Lacking

The Department of Homeland Security falls woefully short in the area of cybersecurity, according to a May 26 report by the Government Accountability Office. For more details, see the *Computerworld* news story at

http://www.computerworld.com/governmenttopics/ government/story/0,10801,102489,00.html

and GAO Report GAO-05-434 (78 pp., May 26,2005), which is linked from
http://www.gao.gov/docsearch/repandtest.html

FBI Begins Crackdown on P2P Piracy

In May, the FBI began executing 10 search warrants across the U.S. against members of the P2P filesharing network "Elite Torrents." This marked the first criminal enforcement against the theft of copyrighted material via the Internet. See

http://www.cybercrime.gov/BitTorrent.htm

Secret Service Teams with FBI to Fight Cybercrime with 'Hacker Hunters'

Now that hacking has become the province of organized crime, government agencies are trying to meet the challenge by forming teams of "hacker hunters" to infiltrate, expose, and prosecute cybercrooks. See
http://www.businessweek.com/magazine/content/05_22/ b3935001_mz001.htm

Massachusetts Shuts Down Spam Gang's Websites

One of the world's biggest spam gangs was shut down in May by a court order in Massachusetts. The gangs dealt in online sales of pornography, pills, pirated software, and fake watches. See
http://news.bbc.co.uk/2/hi/technology/4539715.stm

File Snapshots Now Available on Darkwing

New backup capability on Darkwing is fast, painless, and free

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

As we mentioned in the last issue of *Computing News* ("The New NetApp NearStore R200 Filers," **http://cc.uoregon.edu/cnews/spring2005/filers.htm**), the core of Darkwing is really a pair of new Network Appliance R200 network attached storage units (the NetApp filers).

One of the special features of the new NetApp filers is their ability to take periodic read-only "snapshots" of the filers' contents, thereby providing protection against accidental file loss. While we've always done backups to magnetic tapes stored locally and offsite (and we continue to do so now), those mag tape backups were only taken once a day, and were really meant as insurance against catastrophic system failure rather than as a convenient "safety net" capable of easily handling backup and restoration of individual user files.

Reflecting that intent—as well as the staff time required to consult with users to determine what was lost, plus the time to retrieve, mount, and scan the tapes and then restore the files to disk—charges for file restoration from system mag tape backups have always been steep.

Moreover, retrieving a file from magnetic tape could potentially be delayed for days at a time, depending on when a given file happened to be lost. For example, a file that was accidentally deleted late on a Friday would generally not be able to be restored until Monday morning at the earliest.

The backup situation on Darkwing has improved significantly with our new filers' ability to take snapshots. Snapshots are fast, painless, and free—a great safety net we're happy to make available for your use on Darkwing. Now you can "go back in time" and transparently retrieve copies of files that remain unchanged from the way they appeared hours or days earlier. You can also recover accidental file deletions, botched editing sessions, and most other routine file-related misadventures, unaided and at your own convenience.[1]

Historical snapshots of your files are stored in a read-only `.snapshot` ("dot snapshot") subdirectory on your account, a subdirectory that's located immediately under your default home directory. If you'd like to see what that subdirectory looks like, log into Darkwing using *ssh* [2] , then type:

`% cd $HOME/.snapshot` <— *change to the* **.snapshot** *directory*
`% ls -la` <— *see what files/directories are there*

You'll notice that the `.snapshot` subdirectory has a series of additional subdirectories:

1. **hourly snapshots:**
   `hourly.0`, `hourly.1`, `hourly.2`...through `hourly.26`, representing the most recently taken snapshot (`hourly.0`) all the way down to a snapshot that was taken 26 hours ago (`hourly.26`)
2. **nightly snapshots:**
   `nightly.0`, the most recent nightly snapshot, through `nightly.29`
3. **weekly snapshots:**
   `weekly.0`, the most recent weekly snapshot, through `weekly.3`

When it's time for a new snapshot to be taken, each of the existing directories gets rotated, meaning each directory is renamed and moved. For example, when a new hourly snapshot is taken:

1. the oldest snapshot (`hourly.26`) goes away
2. the old `hourly.25` becomes the new `hourly.26`
3. the old `hourly.24` becomes the new `hourly.25`, and so forth, with the most recently taken hourly snapshot becoming the new `hourly.0`

A similar process happens for the nightly snapshots each night, and for the weekly snapshots each week.

NetApp makes snapshots in a very nimble and efficient way, taking advantage of the fact that while you may have hundreds or thousands of files in your account, most of them don't change very often. This allows the filer to simply store *pointers* to content, plus a relatively modest set of file changes, rather than physically replicating *all* your files on a character-for-character basis every time a snapshot is taken. (For more information about how snapshots work, see "Snapshot™ Technology," **http://www.netapp.com/products/software/snapshot.html**)

Restoring a File From a Snapshot

Assume that over a course of a week or so you created a data file on Darkwing called `mydata.txt` with several thousand observations, entering a few hundred observations per day. While doing final editing on that dataset you accidentally made a catastrophic mistake, a mistake that ruined hundreds of observations. Moreover, assume you failed to notice that mistake before you saved your file (although that devastating mistake quickly became apparent as soon as you began to do your analyses). What to do?

If `mydata.txt` was okay as of the snapshot that occurred an hour or so ago, you could simply restore a clean copy of the file from the snapshot. (To avoid confusion, let's call the restored version of that file `mydata2.txt`).

Begin by logging into Darkwing securely via *ssh*. Then type:

`% cd $HOME/.snapshot/hourly.0` <— *change to the snapshot directory*

`% cp  mydata.txt  $HOME/mydata2.txt` <— *copy the snapshot copy to your normal default directory*

`% cd $HOME` <— *change to your default directory and begin using the recovered file*

Need an earlier version? Restore the file from `hourly.1` or `hourly.2`, (or from `daily.0`, `daily.1`, etc.) instead of from `hourly.0`

What You Should Know About Snapshots

1. **Snapshots are immutable:** you can't change or delete files that are in your `.snapshot` directory any more than you can go back in time and unring a bell once it's been rung. This means, for example, that you can't edit files stored in snapshot directories. You must copy the file to your normal (non-snapshot) space first, and then edit it there.
2. **This service is experimental and is being provided on an as-is basis.** While we anticipate snapshots will continue to be routinely available for the foreseeable future, this *is* a new service and we're currently feeling our way with it just as you will be. As is true with any experimental service, unanticipated circumstances may make it necessary for us to substantially modify or even discontinue the service at any time and without prior notice. For example, if we unexpectedly run short of disk space, we might need to reduce the frequency with which snapshots are taken, or keep fewer generations of snapshots.
3. **You'll always need more than one backup plan.** In spite of the additional protection that snapshots provide, it is always a good idea to back up critical data in multiple locations to provide extra protection against accidental loss.

If you're a UO user and have questions or comments about data snapshots on Darkwing, please feel free to contact me by writing *joe@uoregon.edu* We'd love to hear what you think about the new snapshot facility.

Notes:

[1] Obviously, a user can restore a file from a snapshot only if (a) that file was on the filer long enough to be captured as part of a snapshot, and (b) the restoration is done while the snapshot is still available online.

This means that if you rapidly create a file and then accidentally delete it before it's been around long enough to have a snapshot made of it, the file cannot be restored from a snapshot.

Similarly, if you accidentally delete a file and then go abroad for three months, when you return the following quarter, the file's snapshot will no longer be available (although you may still be able to pay a fee to have the file restored from tape backups by Systems staff).

[2] If you don't know how to log in securely, please see the instructions at **http://micro.uoregon.edu/security/ssh/**

Clarinet (YellowBrix) News Service Dropped

Change takes effect July 31

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

The UO has traditionally offered the clari.* Usenet groups via the university's Usenet servers. However, due to both the myriad new ways that online news from major news sources is being disseminated these days, as well as limited readership of clari.*, we will be discontinuing clari.* Usenet service this summer.

If you have traditionally relied on clari.* for access to breaking news from traditional news media sources, we encourage you to check out the following:

- Google News
  http://news.google.com/
- Online news web sites such as those from
  - CNN (**http://www.cnn.com/**)
  - BBC (**http://www.bbc.co.uk/**)
  - *The New York Times* (**http://www.nytimes.com/**)
  - Yahoo (**http://news.yahoo.com/**)
  - Reuters (**http://www.reuters.com/**)
  - *The Washington Post* (**http://www.washingtonpost.com/**)
- An RSS-based news "feed" such as that offered by Yahoo (see **http://news.yahoo.com/rss**)

Firewall Forget-Me-Nots for Network Administrators:

Before deploying a new firewall, network administrators must keep a number of key points in mind

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

Network administrators who are setting up firewalls for the first time can sometimes encounter problems that they have never seen before. Because a firewall is usually deployed at a critical point within the network infrastructure, these problems can quickly take on a high degree of importance. In this article, we discuss a few of the more common pitfalls an administrator might encounter when performing a new firewall deployment.

Least Privilege

The concept of "least privilege" is one of the most important concepts in computer security. Simply put, the idea of least privilege is that you should provide no more access to a network resource than is absolutely necessary to perform the task at hand. In the case of firewall deployments, this concept is usually implemented by creating distinct network segments or zones: an outside zone, a DMZ or buffer zone, and a private zone.

The DMZ segment (demilitarized zone or buffer zone) is used to allow for access from the outside zone to services that are required by the public at large. Public websites and email relay servers are some of the things you would expect to see on a DMZ. To guarantee least privilege, only the incoming connections that are required to provide for those specific services are permitted to reach the DMZ, while all other incoming connections are blocked.

A private local network segment is also usually required, in order to provide a network segment that has even greater security than the DMZ. This is the local network segment. No incoming connections to this segment are allowed. If a public service is required, administrators must relocate that service to the DMZ. Administrators can significantly weaken their security when they punch holes in a firewall rule set that opens access to services on the private network. For example, if incoming connections are allowed for web servers on the private segment, a firewall loses much of its effectiveness.

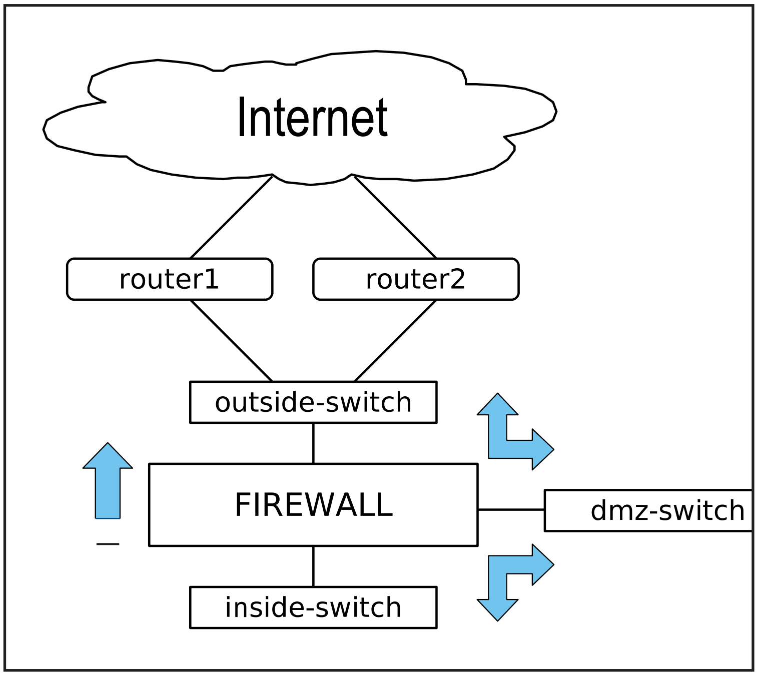


Fig. 1: Standard topology for firewall with DMZ

Rule Set Specifications

Firewall rules are usually thought of as "tuples." A tuple is a triple consisting of a source IP address range, a destination IP address range, and a destination application service type. For example, suppose our DMZ subnet is addressed 111.111.111.0/255.255.255.0. To permit access to all of the web servers on the subnet, a firewall rule could be created that says: ANY, 111.111.111.0/255.255.255.0 http. A thorough understanding of IP addresses and subnet masks is required in order to formulate these rules.

Specifying firewall rules can be somewhat more complicated than simply specifying "source, destination, and port." First, a specific protocol needs to be specified. In this case, the TCP protocol is being used. In addition, the range of values allowed for the source port has been left unspecified. Typically this will be set to either 0-65535 or 1024-65535. And finally, direction needs to be specified. Direction can be incoming, outgoing, or reference specific zones created by the firewall. For example, direction can be FROM the private segment TO the external segment, or FROM the private segment TO the DMZ segment. Finally, the action taken by the rule needs to be specified. A rule action might be any of the following: accept, reject, deny, tunnel, log.

Most firewalls provide an interface that allows for the creation of these rules. In the absence of a hardware GUI interface, a spreadsheet can be used for drafting rule sets. All of the fields can then be specified: description, source zone, destination zone, protocol type, source address range, source port range, destination address range, destination port range, and action.

Description	From Zone	To Zone	Protocol	Source Address	Source Port	Destination Address	Destination Port	Action
Mail	Outside	DMZ	TCP	ANY	ANY	Mail-Server	25	ACCEPT
Mail-Ident	Outside	DMZ	TCP	ANY	ANY	Mail-Server	113	ACCEPT
Web	Outside	DMZ	TCP	ANY	ANY	Web-Server	80	ACCEPT
FTP	Outside	DMZ	TCP	ANY	ANY	FTP-Server	21	ACCEPT
Outbound	Inside	Outside	ANY	ANY	ANY	ANY	ANY	ACCEPT

Note: *In all of these examples, we are assuming that a stateful-inspection firewall is being used. Stateful-inspection firewalls track network connections by recognizing the start of a connection, and allowing return traffic in the opposite direction that is related to the initial connection. This capability makes it much easier to generate firewall rule sets, since only the initial connection direction needs to be specified; control of the return traffic is handled automatically. In contrast, packet-filtering firewalls require specific rules for each direction of any connection.*

Firewalls typically also have an implicit set of capabilities that the administrator must be aware of. These kinds of behaviors can be confusing to someone who is not familiar with the particular brand of firewall that is being deployed. For example, there may be a “default DENY” rule that exists within the firewall, but which is not listed in the GUI. Additionally, the order in which rules are processed can sometimes be opaque. All of these things must be understood if policy is going to be implemented correctly.

Simple Network Protocols

A firewall is a device that filters network traffic. In order to understand if a firewall is operating correctly, one must also understand something about how network traffic travels across the network under normal circumstances. Some of the network protocols that should be understood are: ARP, ICMP, and DHCP.

ARP

The ARP protocol is a layer-2 protocol, that is, a protocol that operates below the IP layer. ARP stands for Address Resolution Protocol. ARP is used by the devices on a local network segment for communication; it is the mechanism that is used to translate 32-bit IP addresses into the 48-bit Ethernet hardware addresses that are hard-coded into network interfaces, and that are used for local Ethernet communication.

Problems relating to ARP usually occur during the initial deployment of a firewall, and they occur on devices that are not updating their ARP caches correctly. For example, if a firewall is deployed in routed mode, it may end up taking the place of the IP address that was previously in use by the router interface. In this case, the ARP mapping for all devices behind the router should automatically update their mapping for that particular IP address almost immediately after the new firewall is put in place. If a host behind the firewall has an old mapping stuck in its ARP cache, it may not be able to send packets through the firewall. It will be able to communicate with local hosts, but will not be able to send traffic through the firewall.

In almost every case, a reboot of a device will force the device to clear its ARP cache. In some cases, commands can be used to manually clear the cache of a device. This problem is usually seen on older machines, and on some networking equipment. In most cases, cache entries automatically time out, and are updated fairly quickly.

DHCP

DHCP is the Dynamic Host Configuration Protocol. DHCP is used to automatically assign network information to devices. This information usually includes IP address, subnet mask, gateway address, domain name, and the location of DNS servers. It is commonly the case that an organization will have a few DHCP servers that are centrally managed to enable handing out this kind of information. Not all machines require DHCP. Some machines rely on DHCP to be able to boot and to continue to retain a fully functioning IP address; other machines may have their network information statically configured and will not utilize DHCP.

During the design of a new firewall installation, the administrators will have to determine how they wish to handle DHCP. In a transparent firewall configuration, the firewall usually does not interfere with the operation of the DHCP protocol. In a routed firewall configuration however, the firewall is usually configured to operate as a DHCP relay agent—that is, an intermediary who passes on DHCP requests to the central servers. In a NAT configuration, the firewall itself may be configured to operate as a DHCP server, and will be configured to hand out private addresses to machines on the local subnet. Usually the mode of operation of the firewall will dictate which of the above choices is made with respect to the operation of DHCP.

The most interesting of these modes of operation is the transparent mode. Administrators must be careful to avoid crafting firewall rules that interfere with the operation of DHCP. Since initial client requests are sent to a broadcast address, such as 255.255.255.255, and may also contain a private address or an initial address such as 0.0.0.0, it is easy to mistakenly block these types of addresses in firewall rules. One of the first tasks that an administrator will perform after installing a new firewall is testing the correct operation of DHCP by booting a dynamic client machine.

Failure to allow for local DHCP relay agents is another common problem in transparent mode installations. The initial DHCP relay responses may come from either a virtual interface address of the router, or from the actual IP address of the router. This is a common occurrence in networks where redundant routers are being used. For example, a local client might expect to receive initial DHCP replies from the IP address 111.111.111.1, or from 111.111.111.2 or 111.111.111.3. Firewall rules need to be designed so that they allow for DHCP replies from the relay agents as well as the central DHCP servers.

ICMP

ICMP stands for Internet Control Message Protocol. ICMP messages are used to pass low-level operational messages across the network. ICMP messages are part of the normal, everyday operation of a network. There are a number of categories and sub-categories of messages, which are referred to as "types" and "codes." Some of the more common types of messages are listed below:

Type	Code	Description
0	0	Echo Reply
8	0	Echo Request
3	0	Destination Unreachable, Network Unreachable
3	1	Destination Unreachable, Host Unreachable
3	2	Destination Unreachable, Protocol Unreachable
3	3	Destination Unreachable, Port Unreachable
3	4	Destination Unreachable, Fragmentation Needed
11	0	Time Exceeded

The most common application that uses ICMP is ping. The ping application is used to send ICMP Echo Request messages to remote hosts to see if they are reachable. In response, the host sends an ICMP Echo Reply message. Another popular application that utilizes ICMP is the trace-route program. Traceroute sends out UDP messages with TTL (time-to-live) settings that are chosen so as to expire at each hop along a network path. An ICMP Time Exceeded message is returned at each hop along the way.

ICMP has been implicated as a source of abuse in a number of situations. Ping can be used by an attacker to do reconnaissance, to send incoming ICMP Echo Requests which show which hosts are reachable on the network. In more serious cases, ICMP has been abused through the transmission of unusually crafted packets that can cause a remote host to crash, a ping-of-death. Other attacks have been performed that utilize spoofed source addresses and local network broadcast destination addresses to cause ICMP traffic flooding.

The most common error that a firewall administrator can make when dealing with ICMP is to assume that all ICMP should be blocked. Outgoing messages such as Echo Request are always allowed. But a number of incoming messages such as Echo Reply, TTL Exceeded, Port Unreachable, and Destination Unreachable need to be allowed for applications to continue to function normally. For this reason, ICMP is usually handled by selectively blocking a few, but not all, of the incoming message types. Blocking incoming ICMP Echo Requests is a common practice. And special features that are designed to prevent ping-of-death and directed-broadcast attacks can be enabled on most firewalls to deal with the most common sources of abuse.

Complex Network Protocols

Many network protocols operate in a very straightforward manner. A client sends a request, and a server sends a reply. Some network protocols, however, are more complicated than that. A client might send a request to one port, and the server might respond by asking to open a connection on a different port. In addition, more complex network protocols can include IP addresses within their data payloads, which creates a dependency not only upon the originating client address, but also upon the IP addresses contained within the protocol messages.

The most common example of protocol complexity is the FTP protocol. The original design of the FTP protocol operates in a mode known as ACTIVE FTP. The client opens a TCP connection to port 21 on the server, the command port. The server responds by opening a new connection with a source port of 20, the FTP data port, but targets a new destination port on the client. Early packet filters and firewalls were not able to recognize that these incoming connections were related to the original client requests. The creation of a PASSIVE FTP mode, where connections are always initiated from the client side, went a long way towards resolving this issue. At this point, most firewalls are capable of supporting either mode of FTP.

A particular brand of firewall may or may not support protocol filtering for one of the more complex protocols. For this reason, it pays to plan ahead when choosing a firewall platform. Administrators who plan on using NAT (network address translation) need to pay particular attention here since private addresses can add an additional layer of complexity to the handling of these types of protocols. Some of the protocol types to be aware of are: RTSP (Real-Time Streaming Protocol for RealAudio, QuickTime, and IPTV), SQL*Net (oracle), H.323 (Netmeeting, CU-SeeMe, and VOIP), SIP (Session Initiation Protocol), and TFTP.

Spotlight on Security

Latest MyTob Email Worm Mimics Phishing Scams to Infect PCs

The latest variants of the MyTob worm attempt to trick email recipients into clicking on an embedded link to a malicious website. The emails appear to be legitimate warnings from an IT department or ISP about a problem that's been found with the recipient's email account.

Only Windows PCs are vulnerable to MyTob infection. For more details, see
http://www.theregister.co.uk/2005/06/08/mytob_phishing_worm/

Apple Releases Patches for Tiger, Panther

On June 8, Apple released 11 patches for vulnerabilities in OS X Panther 10.3 and OS X Tiger 10.4. The most serious of these could allow buffer overflow attacks and give hackers root access, enabling the execution of malicious code.

For more details, see
http://www.macnewsworld.com/story/43717.html

Veritas Hole Draws Attacks

A software bug first noted in March has begun biting systems running unpatched versions of Veritas Backup Exec Software.

The affected software triggers backups of data files on Windows servers in case of computer crashes or other emergencies. It is a critical component of many corporate and government computer systems. If left unpatched, systems running Veritas Backup Exec are vulnerable to hacker attacks that run malicious code.

The patches are available from Veritas' patch summary site at **http://seer.support.veritas.com/docs/277429.htm**

For more details, see
- "Veritas Security Flaw Attacked" at
  http://www.technewsworld.com/story/44353.html

- US-CERT Technical Cyber Security Alert TA05-180A
  http://www.us-cert.gov/cas/techalerts/TA05-180A.html

Netscape 8 Users Advised to Upgrade to Version 8.0.2

The initial release of Netscape 8.0 was marred within the first 24 hours by the discovery of a number of critical vulnerabilities. The company responded by releasing version 8.0.2, which fixes the problems.

For more details, see "Netscape fixes holes in 'security' browser" at
http://www.zdnet.com.au/news/security/0,2000061744,39192767,00.htm

Microsoft Offers Workaround for Latest Critical Internet Explorer Vulnerability

In early July, researchers at SEC Consult discovered a serious new flaw in Microsoft's Internet Explorer that can cause the browser to unexpectedly quit and execute malicious code.

Affected versions include IE 6.0 on Windows 2000 with Service Pack 1, 3 and 4, and on Windows XP with Service Pack 1 and 2. Microsoft recommends disabling the file Javaprxy.dll and refers users to its Workarounds section. For more details, see

- "Microsoft Warns of Unpatched IE flaw
  http://www.zdnet.com.au/news/security/0,2000061744,39200480,00.htm
- "Microsoft Internet Explorer Javaprxy.dll COM Object Execution"
  http://www.securiteam.com/windowsntfocus/5FP010UGAA.html
- Microsoft Security Advisory (903144)
  http://www.microsoft.com/technet/security/advisory/903144.mspx

Security Firms Report Dramatic Increase in Malware As Organized Crime Enters Cyberspace

In the first six months of 2005, nearly 8,000 new pieces of malware—a 60% increase over last year—were detected by the security company Sophos. The biggest growth was in Trojan horse viruses, cleverly disguised malware that spread via email attachments. For more details, see
http://news.zdnet.com/2100-1009_22-5774841.html

Symbian Smartphones Vulnerable to Trojans

A new Trojan known as Doomboot.A can disable Symbian Series 60 smartphones by launching a virus that drains phone batteries in less than an hour. Rebooting the phone can cause data loss. Security company F-Secure has published information on its website that aids users in disinfecting phones attacked by the Doomboot.A virus, known as CommWarrior.B. For more details on the virus, as well as how to disinfect an infected phone, see F-Secures' Doombat.A virus description page at
http://www.f-secure.com/v-descs/doomboot_a.shtml

Secunia Spots Critical Flaws in RealOne/RealPlayer/Helix Player/Rhapsody

On June 24, Secunia security researchers reported highly critical flaws in RealOne Player, RealPlayer, Helix Player and Rhapsody that can be maliciously exploited to overwrite local files or to compromise a user's system. Details and patches are available on the Secunia Advisory SA15806 web page at
http://secunia.com/advisories/15806/

Students Will Soon Be Able to Handle Many of Their UO Financial Transactions Online

Electronic billing and payments, with real-time accounting, revolutionize the way the UO does business

After more than a year of research, planning, and creative programming, the UO is on the cusp of changing the way it does business.

Thanks to the efforts of the Business Affairs office and a programming team from the Computing Center's Administrative Services group, students will soon be able to handle most of their financial transactions online via DuckWeb.

Business Affairs' Assistant Director of Information Systems Mark McCulloch led the effort to make e-bill and e-pay a reality at the university. Building on a prior experience with electronic payments through an arrangement with US Bank, Mark and his group consulted with the Computing Center about the possibility of adding an electronic billing component and making account records accessible through DuckWeb.

After many months of discussion and research involving several groups, including the Banner Coordinating Group and the Computing Center*, followed by approval from the UO's Strategic IT Issues committee, the Business Affairs and Computing Center team decided to work with infiNET, a software company with a proven track record in providing full-service automated billing, payment processing, and commerce solutions designed specifically for higher education.

It was then up to systems analysts Joey Mitchell and Robert Gillespie to integrate the *QuikPAY®* software into the BANNER enterprise system and the DuckWeb server. Their programming assignment was challenging, as entirely new interface modules had to be written in order to integrate seamlessly into DuckWeb.

The *QuikPAY®* system is being phased in with both electronic and paper billing still functioning. Ultimately, electronic billing will completely replace paper billing, but students who wish to continue to receive paper bills may submit a request to opt out of *QuikPAY®*.

Briefly, here's how *QuikPAY®* works:

1. Students may log into their DuckWeb account using their UO ID and personal access code (PAC) and authorize their parents, guardian, or sponsor to view and pay their UO bills (tuition, fees, campus card deposits, loan payments, housing and parking fees, undergraduate application fees, and so on).

   If desired, bills may be printed out from the web in PDF format. The printout contains a scan line that facilitates bank processing.

2. Each billing cycle, students and their authorized payers will receive email notification on how to retrieve their *QuikPAY®* E-bill.

3. Students have complete control over access to their account information: they may change authorized payers at any time and may also restrict viewing access according to their preferences.

The advantages of the new system are considerable. Not only is it extremely convenient, giving students and their authorized payers the ability to access financial account information and pay bills via the Internet at any time, but it will enable significant savings in paper, postage, and staff processing time each year.

One of the most advanced features of the new system is that payments are posted to Banner and updated in *real time*, which means that there is no longer any lag time between the time a bill is paid and the time it's credited to a student's account. It also means that holds placed on a student's registration can be released immediately, when the bills are paid and recorded online.

Another convenience is that parents or other authorized payers who wish to send money to their students can now make secure online deposits to the student's Campus Cash account.

QuikPAY® is fully compliant with all federal privacy requirements as mandated by FERPA (Family Educational Rights and Privacy Act). To learn more about the new *QuikPAY®* system, please see

http://baomail.uoregon.edu/studentservices.htm

** Implementation of QuikPAY® is the result of teamwork between the staff in BAO Student Financial Services and Information Systems, Admissions, and the Computing Center. A lot of time and care went into testing the system, developing informational communication pieces for students, parents, and staff, and analyzing service needs. ASUO representative Katie Wallace also provided valuable feedback for developing our informational materials.*

quick systems status check:

To check on the status of Banner, the Data Warehouse, DuckWeb, web services, and email systems, see

http://status.uoregon.edu/

Spamvertised Drugs and Dubious Medical Devices

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

UO faculty, students and staff, and Internet users in general, are routinely bombarded with spam encouraging them to buy prescription drugs ("pillz") or dubious medical devices from overseas pharmacies.

Products offered this way often include:

- drugs or medical devices of dubious safety or unproven efficacy
- prescription medications dispensed without a legitimate prescription from a licensed physician
- controlled substances (including scheduled narcotics)
- unapproved new drugs

Online purchasers of medical products are at substantial risk. In many cases, overseas pharmacy sites are virtually impossible to trace. When they charge your credit card and ship nothing, you'll have no recourse when your illegal drug purchase fails to arrive.

In other cases, your drug shipments may be detained at the border. Or, if you actually receive the pills you ordered, they may be unsafe for you to take, or they may do nothing to cure a serious illness or condition.

The Big "Personal Importation" Myth

Many spammer "pillz" sites will tell you that you can freely import drugs or medical devices into the United States for personal use. However, in many cases that is simply *not* true. The Drug Enforcement Administration and the Food and Drug Administration have issued written guidelines to travellers and potential Internet drug purchasers outlining what's allowed, and Customs, DEA, and FDA personnel have received extensive lists of drugs and medical products that are to be summarily refused entry.

Thus, if you attempt to purchase drugs or medical products from overseas spamvertised sources, you may find your purchase seized at the border by Customs, potentially leaving you out-of-pocket the amount you'd paid—as well as potentially leaving you liable for fines, penalties, or even arrest as a drug smuggler.

Don't be taken in by Internet medical fraudsters: if you have a medical condition, see a licensed physician and fill any prescription he or she gives you only at properly licensed reputable pharmacies.

Never buy *any* product from spammers, particularly potentially unsafe or dubious drugs or medical devices. You may be ripped off outright, or if the overseas spammer does attempt to make a shipment to you, your purchase may never make it past the border.

For more information, please see:

1. Dispensing and Purchasing Drugs On-line
   http://www.deadiversion.usdoj.gov/faq/internetpurch.htm
2. Customs and Border Protection Medication/Drugs
   http://www.customs.gov/xp/cgov/travel/alerts/medication_drugs.xml
3. FDA Traveler's Alert
   http://www.fda.gov/ora/import/traveler_alert.htm
4. FDA Personal Importations Web Site
   http://www.fda.gov/ora/compliance_ref/rpm_new2/ch9pers.html
5. FDA Office of Regulatory Assistance Import Program
   http://www.fda.gov/ora/import/default.htm
6. IA #66-41 - 9/28/00 Revision of Import Alert #66-41 "Unapproved new drugs promoted in the U.S." attachment revised 6/2/05
   http://www.fda.gov/ora/fiars/ora_import_ia6641.html
7. IA #80-06 - 9/28/92, Automatic detention of fraudulent and deceptive medical devices," attachment revised 2/10/04
   http://www.fda.gov/ora/fiars/ora_import_ia8006.html

« more sites worth seeing »

1. **New Architecture Project…** Technical reports from this DARPA-funded research project for creating a new generation of Internet architecture:
   http://www.isi.edu/newarch/
2. **2005 Global Financial Security Survey…** Deloitte's third annual report, which compiles information from IT security teams around the world:
   http://deloitte.com/dtt/research/0,1015,sid=1013&cid=85452,00.html
3. **The Interactive Nolli Map Website…** See the map that won this year's Outstanding Project award from the NorthWest Academic Computing Consortium (NWACC):
   http://nolli.uoregon.edu/
4. **The Prolexic Zombie Report…** What are the top 20 most infected networks on the Internet? Learn more about attempted large-scale DDoS attacks at:
   http://www.prolexic.com/zr/

Processing a Sorted SAS Dataset: the FIRST

The BY statement is more versatile than you might think…

Robin High
Statistical Programmer and Consultant
robinh@uoregon.edu

In SAS, DATA and PROC steps consist of series of statements which often begin with a keyword and always end with a semicolon. The statement that begins with the keyword BY followed by a list of categorical or integer variable names has several important functions, including:

- it sorts a dataset with variables it contains through PROC SORT
- it processes data by subgroups in statistical procedures
- within the DATA step it allows records to be merged or updated from two or more datasets linked together by common ID variables

However, the BY statement entered into a DATA step has one very important application that is not as well known or understood: it gives SAS the ability to process data included in one dataset where the records are organized by combinations of levels of classification variables.

Suppose an existing SAS dataset contains one or more variables coded as character data or integers with a finite number of values. The dataset can be organized into blocks of records or subgroups defined by the unique combinations of categorical or integer values. Within these defined subgroups you can process all records of this dataset with a DATA step itself.

For example, consider a hypothetical dataset called `survey` which contains the following variables to identify groups of records: `Gender` (coded here as `gndr` with `m=male` and `f=female`) and the category `age` (coded as integers 1, 2, and 3 to represent three distinct age groups). `Score` was computed from the summation of several Likert scale responses given by each person:

```
DATA survey;
LABEL gndr='Gender';
INPUT id $ gndr $ age score @@;
CARDS;
b f 1 30 g m 1 27 l m 2 39 c f 2 23 h f 3 37
e m 1 49 n m 2 25 o m 3 38 a f 1 28 k f 3 32
d m 1 41
;
```

First, sort the dataset with PROC SORT by `gndr` and `age` (in ascending order). The unique ID for each record is also included on the BY statement as the third variable listed to organize the dataset, even though it is not required for subsequent data processing illustrated here:

```
PROC SORT DATA=survey;
BY gndr age id;
RUN;
```

Following PROC SORT is a DATA step that writes a new dataset called `sum_var`. Enter a BY statement following the SET statement (which reads the sorted dataset called `survey`) to indicate the records in the dataset have been sorted by `gndr` and `age`. Since the objective is to process the data across all records identified by levels of gender or across all records for both gender and age, the ID variable does not need to be included on this BY statement:

```
DATA sum_var;
SET survey;
BY gndr age;
<enter additional DATA step statements - see below>
RUN;
```

These three statements give SAS the capability to identify the first and last record within each subgroup of records defined by the variables on the BY statement. This feature of the DATA step has many helpful data processing applications, but only one will be described here to illustrate how it works.

In order to process a sorted dataset with the DATA step, SAS automatically assigns two internal variables for each variable listed on the BY statement which are dummy coded as 0/1 to represent a false/true condition. For gender, the variable is called `FIRST.gndr` and is equal to 1 to identify the first record of each subgroup defined by the sorted values of gender; otherwise, it is assigned a value of 0. A second variable called `LAST.gndr` is equal to 1 for the last record of each value of gender in each subgroup; it is assigned 0 otherwise. Analogous variables are computed internally for the three levels of age. These variables are not included in the new dataset; they only exist to help SAS identify the first and last records of the subgroups into which the records have been sorted.

You'll recall that the survey dataset described above was sorted by `gndr`, `age`, and `id`. Below you'll find the sorted dataset of values for `id`, `gndr`, and `age` variables followed by the respective "internal" values of `FIRST.<var>` and `LAST.<var>`, and a `score` variable with which SAS will calculate some summary statistics.

Because only two values of gender exist that were listed first on the BY statement, the columns for `FIRST.gndr`

and LAST of DATA Step Processing

and LAST.gndr each contain only two 1's. However, since age is sorted within each level of gender, its associated FIRST and LAST variables change much more often (as indicated by the larger number of 1's in the respective columns). If there is only 1 record for a group defined by age, both FIRST and LAST values equal 1 (as is the case for gender=m and age=3).

id	gndr	FIRST.gndr	LAST.gndr	age	FIRST.age	LAST.age	score
a	f	1	0	1	1	0	28
b	f	0	0	1	0	1	30
c	f	0	0	2	1	1	23
h	f	0	0	3	1	0	37
k	f	0	1	3	0	1	2
d	m	1	0	1	1	0	41
e	m	0	0	1	0	0	49
g	m	0	0	1	0	1	27
l	m	0	0	2	1	0	39
n	m	0	0	2	0	1	25
o	m	0	1	3	1	1	38

The dataset survey can now be considered to contain both the actual data values and the internal values SAS assigns. As a result, you can process the records defined by variables listed on the BY statement with IF statements entered in the DATA step. One simple example to demonstrate how this data processing works is to accumulate counts and sums in the DATA step for all persons across values of age for each level of gender:

```
DATA sum_var;
SET survey;
BY gndr;
DROP id score age;
RETAIN gndr_sum gndr_count;
IF (FIRST.gndr EQ 1) THEN
 DO; gndr_count=0; gndr_sum =0; END;
gndr_count = gndr_count + 1;
gndr_sum = gndr_sum + score;
IF (LAST.gndr EQ 1) THEN
 DO; gndr_mean = gndr_sum/gndr_count; OUTPUT;
END;
RUN;
```

The purpose of these two IF statements should not be confused with a statement such as "IF gndr EQ 1 then…" (which is incorrect since gender itself is character data that can only equal 'f' or 'm'). The actual values of gndr are not referred to; the value "1" entered above refers only to the answer to the question that is asked for each record: "Is this record the first (or last) of a group of records sorted by gender?"

The objective of this DATA step is to accumulate summary statistics by values of gender. When the first record in any subgroup is encountered (e.g., FIRST.gndr = 1), the summary statistics must be set to 0. Also, any new variables computed within the DATA step should be included in a RETAIN statement since all computed variables are automatically set to missing whenever the SET statement reads a new record.

Records should only be output to the new dataset called sum_var when LAST.gndr equals 1, so the inclusion of an OUTPUT statement must follow "IF LAST.gndr". Since values of score, id, and age are no longer relevant, their names are entered on the DROP statement.

```
PROC PRINT DATA=sum_var NOobs Label;
RUN;
```

```
Gender   gndr_sum   gndr_count    gndr_mean

  f        150          5           30.0
  m        219          6           36.5
```

PROC MEANS would be a more natural and efficient procedure to make the computations of this particular example and to collect other summary statistics. However, these statements demonstrate the versatility of processing data tasks you can perform within a DATA step that includes sorted BY variables. It essentially allows you more control and the ability to delete or modify records with additional statements.

A few situations where this approach has proved most helpful are:

- to delete single records from a dataset that should exist as pairs
- to transpose a dataset and make computations
- to assign values from lagged variables within subgroups

The short example presented here is one of many illustrations of why the SAS DATA step is a very powerful component of the SAS system. Along with arrays, FIRST and LAST data processing can be among the most difficult concepts to grasp. However, when you start to think of data processing by subgroups, the BY statement entered into the DATA step can become a commonly applied feature for which you will find many applications.

« sites worth seeing »

1. **"How to Stop Spam"…** The AOL postmaster gives his take on spam remedies, placing maximum responsibility for spam-busting on the doorstep of messaging providers:
   http://www.circleid.com/article/917_0_1_0_C/

2. **Section 508 web accessibility standards…** Test your website's compliance with federally mandated accessibility standards:
   http://bobby.watchfire.com/bobby/html/en/index.jsp

3. **Cyberinfrastructure Technology Watch…** Get the latest news, ideas, and information on cyberinfrastructure technology, and join the discussion. If you're interested in high-performance research computing, this site is for you:
   http://www.ctwatch.org/

4. **"Google Zeitgeist"…** Check out this regularly updated page to track the searching trends of Google users. Among other trends, this site lists the top ten queries in a number of categories over a given period of time (weekly, monthly, and annually):
   http://www.google.com/press/zeitgeist.html

5. **End-user phishing information…** A list of informational sites on phishing compiled by UO computer support staff:

   Anti-Phishing Working Group: **http://www.antiphishing.org/**

   "How Not to Get Hooked by a Phishing Scam":
   http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

   "Help prevent identity theft from phishing scams":
   http://www.microsoft.com/athome/security/email/phishing.mspx

   "IT tackles phishing":
   http://www.infoworld.com/article/05/01/21/04FEphishing_1.html

   "Avoiding Social Engineering and Phishing Attacks":
   http://www.us-cert.gov/cas/tips/ST04-014.html

   "Online U: The Mission-Critical Web, 'Phishing' Attacks and You":
   http://duckhenge.uoregon.edu/io/article.php?id=155

   "Some Technical Suggestions for Institutions Targeted by Phishers":
   http://darkwing.uoregon.edu/~joe/antiphishing/phishing-suggestions.pdf

6. **"Spam 2005 Technology, Law and Policy"…** A dozen papers surveying the anti-spam efforts of policy makers, ISPs, and technologists:
   http://www.cdt.org/speech/spam/spam2005/

7. **UO's Instructional Technology Directory…** A new web resource designed to help instructors identify and locate educational technology support services that meet their teaching needs:
   http://itdirectory.uoregon.edu/

8. **Scirus…** A search site for scientific information only:
   http://www.scirus.com

9. **"A quick and dirty intro to Nessus"…** A Flash animation demonstrating how this open-source vulnerability scanner works:
   http://www.irongeek.com/i.php?page=videos/nessus

10. **Technical interest groups on campus…** Useful links to discussion groups for managers of UO PC and Mac labs, departmental tech support personnel concerned about campus computing security, and those who support Macintoshes on campus:
    http://deptcomp.uoregon.edu/resources.html

Virus Analysis Sites

In the Spring 2005 *Computing News* (**http://cc.uoregon.edu/cnews/spring2005/virustotal.htm**) we briefly explained how you could submit a suspicious attachment to VirusTotal (**http://www.virustotal.com/**) for scanning and identification by several antivirus products. Because of the interest in that article, we wanted to call attention to two other helpful virus information sites:

- Jotti's Malware Scan (similar to VirusTotal): **http://virusscan.jotti.org/**
- Norman's Sandbox Information Center (a more extensive detection system): **http://sandbox.norman.no/**

More on Norman's Sandbox: For those who may not be familiar with the concept of a "sandbox," it's a carefully isolated facility that allows you to test potentially dangerous programs in a controlled and well-equipped lab environment. By using a sandbox, you can learn what a virus might do in the wild without any possibility of its escaping and wreaking havoc on real systems or the Internet.

Norman's sandbox web interface allows you upload a suspicious file for examination and sends a report by return email with information about what it saw, including:

- identity of the virus found, if any
- any files created or modified by the virus
- any registry values created or modified by the virus
- any process startup information (e.g., "will automatically restart after boot," etc.)
- a listing of the host or hosts that the virus may be attempting to contact to register itself with its controller, download updates, receive denial of service targeting instructions, and so on

The sandbox site also allows you to search a database of samples that others have previously submitted. The Norman Sandbox website is a real resource, almost like having your own malware analyst on site.

Please Tell Us How You Get Help with Computing and Networking Questions

As part of the Computing Center's 2005/2006 planning initiatives, we committed to looking at how users currently get help with their computing and networking questions in order to determine if there are ways we could simplify or improve that service.

Please help us with that project by sharing your opinions about the following questions:

1. **Are you faculty, student or staff?**

a) UO faculty member
b) UO staff person
c) UO graduate student
d) UO undergraduate student
e) other (please specify) ______________________

2. **How would you describe your level of computing and networking expertise?** (Circle one)

a) I'm an expert
b) I'm not an expert, but my skills are above average
c) I'm an average user
d) I'm a novice or beginning user

3 **When you have a computing or networking question, can you usually get your question answered?** (Circle one)

a) always (or virtually always)
b) usually
c) sometimes yes, sometimes no
d) usually not
e) never (or virtually never)
f) not applicable

4) **When you have a computing or networking question, what is your *preferred way* to seek help?** (Circle one)

a) email
b) telephone
c) face-to-face/ in person
d) check web pages or other online documentation
e) check books/manuals/printed documentation
f) other (please specify)

____

5. **Focusing on your *preferred way* to seek help, and thinking about both the quality of the response you receive and the speed with which you receive it, does the UO do a good job of providing computing and networking help to you?** (Circle one.)

a) help is excellent
b) help is above average
c) help is average
d) help is below average
e) help is poor or non-existent

6. **Thinking for a moment about support that happens by telephone or by email, some users prefer to be able to directly contact an appropriate party. Others prefer to have a single number to call or a single email address to write for support. Which do you prefer?** (Circle one)

a) I prefer to be able to directly call or email the appropriate party
b) I prefer to have a single number or single email address to contact
c) other (please explain)

____

____

7. **If you prefer a single number or single email address for help, please indicate which current help resources you'd like to see consolidated under a single contact number. (**Check ALL the resources you'd like to see consolidated under a single number):

___ general Computing Center number (**x6-4403**)
___ current Microcomputer Help line (**x6-4412** or *microhelp@lists.uoregon.edu*)
___ current large systems consulting help line (**x6-1758** or *consult@uoregon.edu*)
___ current Network Services hotline (**x6-4395** or *nethelp@ns.uoregon.edu*)
___ Documents Room in McKenzie Hall (**x6-4406**)
___ operator in the CC machine room (**x6-4382**)
___ electronics repair shop (**x6-3548**)
___ help line for Telecom Services (**x6-1023**)
___ phone numbers for Computing Center-managed computing labs such as CC-EMU (**x6-1769**), CC-McKenzie (**x6-0787**), CC-Millrace (**x6-0316**), CC-Klamath Lab (**x6-4781**), and so on.
___ phone numbers for the Library ITCs, such as those in the Knight and Science Libraries
___ phone numbers for departmental computing support *personnel*
___ phone numbers for departmental computing *labs*
___ other (please specify):

____

____

- OVER

Survey, continued…

8. Thinking now about the availability of support, do we have help available when you have questions?

a) yes, current coverage is sufficient

b) no, more coverage is needed (please describe the period that needs more coverage, e.g., nights, weekends, early morning, 24 x 7 coverage, etc.):

____

____

9. Is there a type or kind of consulting support we don’t currently offer that you need? For example, do you need help with a particular piece of software or a particular task perhaps? If so, what would that be? (Please describe.)

____

____

10. What else can we think about doing to improve our ability to help you with your computing and networking questions?

____

____

Please return this questionnaire to:

Help Desk Questionnaire
Computing Center
University of Oregon
Eugene, OR 97403

Thanks!

SAS Notes

1. New Feature of SAS 9.1.3: Read & Write Excel Worksheets

SAS 9.1.3 allows you to read Excel worksheets directly rather than entering PROC IMPORT commands. Data must be formatted in a consistent manner down columns with variable names in the first row. In the example below, SAS identifies a worksheet named `Sheet1` as the literal name ‘`Sheet1$’n`.

The following DATA step reads two worksheets with an identical file structure from one workbook and appends them into a single SAS dataset called `sas_data`:

```
LIBNAME exbk excel ‘c:\your_file.xls’ ver=2000;
DATA sas_data;
SET exbk.’Sheet1$’n exbk.’Sheet2$’n;
RUN;
LIBNAME exbk clear;
```

With the second LIBNAME statement, SAS releases control over the Excel workbook, allowing you to access it once again from Excel. Data may also be written to an Excel file with the DATA step:

```
DATA exbk.pred;
SET predicted;
RUN;
```

The two LIBNAME statements above need to be entered and the worksheet is named ‘pred.’ However, the Excel file must not already exist, since this approach does not include the REPLACE option

2. SAS/PC Requires XP Pro

Prospective UO users of SAS/PC should note that it requires XP Professional rather than the XP Home edition of the Windows operating system. (Note: SAS/PC will run on other PC operating systems, such as Windows 2000, but XP users who wish to install SAS must run XP Professional.)

SUMMER WORKSHOPS

This is the last season for open-enrollment information technology (IT) workshops, which are being replaced this fall with *Workshops on Demand* (see below).These workshops are free and open to currently enrolled students, as well as staff and faculty. See **http://libweb.uoregon.edu/it/** for course outlines and the most current information, ***Prerequisites are required unless otherwise indicated.***

Workshop	Day/Date	Time	Location	Presenter
Web Publishing, Multimedia ✔Prerequisites				
Web Publishing I… ★✔Prerequisites: Familiarity with a web browser such as Netscape or Internet Explorer and an account on Darkwing or Gladstone (not Oregon!); you must know your username and password				
	Fri July 8	2 PM - 3:50 PM	144 Knight Library	Frantz
	Mon July 11	10 AM - 11:50 AM	144 Knight Library	Munro
Web Publishing II… ★✔Prerequisites: Web Publishing I or equivalent knowledge and skills, and a web page you've created				
	Fri July 22	2 PM - 3:50 PM	144 Knight Library	Jablonsky
	Mon July 25	10 AM - 11:50 AM	144 Knight Library	Harper
Dreamweaver I… ✔Prerequisite: Web Publishing I & II or equivalent knowledge and skills				
	Mon Aug 8	10 AM- 11:50 AM	144 Knight Library	Bell
Dreamweaver II ✔Prerequisite: Web Publishing III and Dreamweaver I (or equivalent knowledge and skills)				
	Mon Aug 15	10 AM- 11:50 AM	144 Knight Library	Smith
Course Websites, Copyright, Presentation & Research Software				
EndNote: What Is It & Why Should I Use It? How to create and store citations, organize and retrieve citations, and format footnotes and bibliographies	Mon July 11	NOON- 1:20 PM	235 Knight	Lenn
Blackboard for Instructors I	Mon June 20	1 PM - 2:50 PM	144 Knight	Johnson
Blackboard for Instructors II ✔Prerequisite: Blackboard for Instructors I or experience teaching with the Blackboard system				
Explore additional features of Blackboard	Mon June 27	1 PM - 2:50 PM	144 Knight	Johnson
Advanced Blackboard ✔Prerequisite: Blackboard for Instructors I or experience teaching with the Blackboard system				
Gradebook setup & debugging	Fri July 1	1 PM - 1:50 PM	235 Knight	Johnson
Advanced techniques for content creation	Fri July 8	1 PM - 1:50 PM	235 Knight	Johnson
Online quizzes and Respondus	Fri July 15	1 PM - 1:50 PM	235 Knight	Johnson
Multimedia on your coursesite	Fri July 29	1 PM - 1:50 PM	235 Knight	Johnson
Preview of Blackboard 6.3	Fri Aug 5	1 PM - 1:50 PM	235 Knight	Johnson

Workshops on Demand

In response to the changing needs of the campus community, the UO Libraries have introduced *Workshops on Demand*, a new model for offering technology training to faculty, staff, and students. These workshops will replace the open enrollment workshops beginning in fall 2005, but members of the UO community can start requesting them now. The new training model will emphasize increased collaboration with faculty in integrating information technology skills into the curriculum. A list of training topics is shown below. See **http://libweb.uoregon.edu/it/ondemand.html** for full details.

Academic Tools and Issues:
- Blackboard for Instructors
- EndNote
- Copyright and Intellectual Property
- Preventing plagiarism
- Classroom technology
- Geographic Information Systems (GIS), including ESRI software products

Communication Tools:
- Email (Eudora, Outlook, Pine, Webmail)
- Mailing lists
- Chat
- Web-based conferencing
- Desktop video conferencing
- Blogs

Graphics and Digital Images:
- Digital camera use
- Photoshop
- Scanning
- Web searching

Web Design and Development:
- HTML, XHTML
- Cascading Style Sheets (CSS)
- Metadata
- Dreamweaver
- Web design principles
- Usability testing
- Accessibility
- PHP
- Web forms, Equations

Document Production:
- Microsoft PowerPoint
- PDF production

Multimedia Production:
- Audio recording and editing (analog and digital)
- Video recording and editing (analog and digital)
- Streaming media (create, index, archive, distribute
- Flash
- CD-ROM mastering
- Reformatting

Research Strategies

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

- microcomputer technical support
- help with computing accounts, passwords
- scanning, CD burning, digital video
- help with damaged disks, files
- system software help
- Internet connections, file transfers
- public domain software, virus protection
- software repair (carry-in only, $80/hour, 1/2 hour minimum)

Documents Room Library

http://docsrm.uoregon.edu/

(175 McKenzie Hall)
346-4406

Modem Number

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

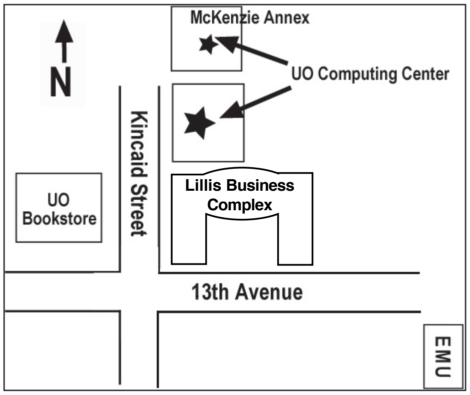
Large Systems Consulting

http://cc.uoregon.edu/unixvmsconsulting.html
(225-239 Computing Center)
346-1758
consult@uoregon.edu

- Unix
- email, multimedia delivery
- scientific and cgi programming
- web page development

Statistics Consulting

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



Electronics Shop (151 McKenzie Hall)

http://cc.uoregon.edu/e_shop.html
346-3548
hardwarehelp@uoregon.edu
Computer hardware repair, upgrades

Network Services

http://ns.uoregon.edu/
346-4395
nethelp@ns.uoregon.edu
Central data communication and network services

Telecommunications Services

http://telcom.uoregon.edu/
346-3198
Local and long distance phone service for UO campus.

Administrative Services

http://ccadmin.uoregon.edu/
346-1725
Programming support for campus administrative computing.

Computing Center Hours

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

McKenzie Building Hours

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

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

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