University of Oregon

COMPUTING NEWS

SPRING 2004

More than a dozen members of the Oregon Nanoscience and Microtechnologies Institute (ONAMI), including representatives from the UO, OSU, PSU, and OHSU, met on campus recently to discuss key projects. Shown here, left to right, are UO physics professor Mike Ramer, Oregon Center for Optics; Dr. Rich Linton (partially hidden), UO Vice President for Research; Professor Ron Sakaguchi, OHSU; Dr. Dave Johnson, ONAMI co-director and UO chemistry professor; and ONAMI executive director Skip Rung. See ONAMI story on page 10.

IN THIS ISSUE...

Time Nears for Migration from Oregon to Darkwing/Gladstone

It's time to move your email and web pages off Oregon and onto Darkwing or Gladstone!

As most of you know, by fall 2004 we will have discontinued service on Oregon, the academic OpenVMS system (administrative users on Daisy and Donald are not affected). This means that users who are currently on oregon.uoregon.edu will need to complete their migration to Darkwing or Gladstone by late summer 2004. For instructions, go to **http://cc.uoregon.edu/cnews/fall2002/mailmove.html**

(**Note to faculty emeritii:** instead of following these instructions, please contact Lucy Lynch at *postmaster@list.uoregon.edu* for help with the migration.)

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

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

- **"The Great Change."** A useful set of tools to help you manage various facets of the migration:

http://darkwing.uoregon.edu/~majordom/great-change.html

- **"Moving Day."** Five easy steps for moving your email to Darkwing and updating your list subscriptions:

http://darkwing.uoregon.edu/ ~majordom/moving-day.html

UNIVERSITY OF OREGON

COMPUTING CENTER

COMPUTING NEWS

VOL. 19 #2

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/

Telephone: (541) 346-1724

Got Extras?

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

UO Employs Grid Technology in High Performance ICONIC Project

To improve medical diagnosis and treatment for brain-related conditions such as epilepsy, stroke, and depression, researchers at the University of Oregon's Neuroinformatics Center are utilizing the power of grid computing.

The UO researchers' goal is to provide doctors and other researchers access to critical patient data on demand via grid computing and supercomputer technology. After receiving a National Science Foundation grant in 2003, the Neuroinformatics group set to work designing the ICONIC Grid (Integrated Cognitive Neuroscience, Informatics, and Computation), which utilizes the collective power of IBM eServer p690, eServer p655 servers and IBM Bladecenter,J20 servers running Linux, WebSphere Application Server, and the open source Globus Toolkit.

The ICONIC Grid was completed earlier this year and campus researchers are continuing to explore its medical applications.

To learn more, see *InformationWeek*'s March 17 report at

http://www.informationweek.com/story/showArticle.jhtml?articleID=18400615

New Online Class Schedule Debuts to Rave Reviews

Try it out: Go to the UO home page at www.uoregon.edu and click on "Class Schedule"

Joyce Winslow
jwins@uoregon.edu

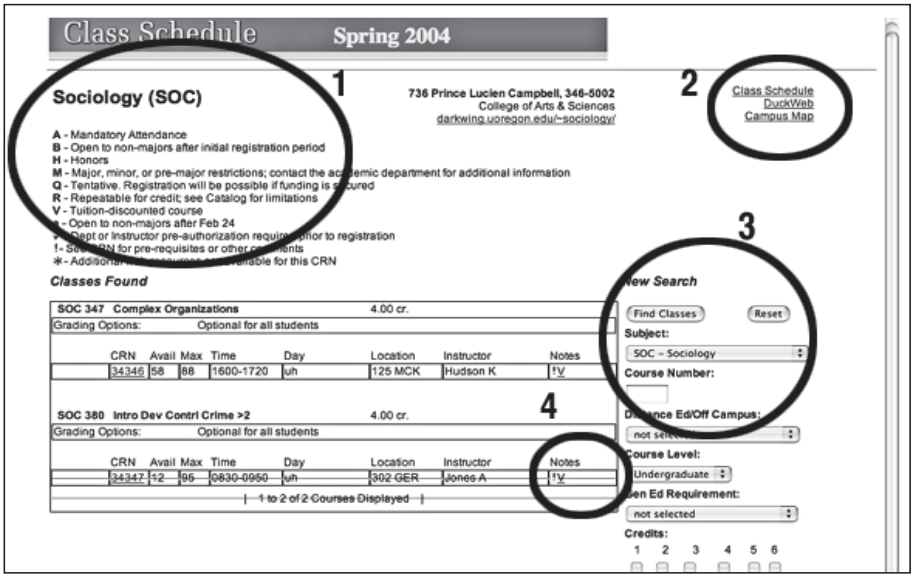
"This is *sooo* cool!"
"I love it!"

These are the kinds of spontaneous comments we've heard recently from students trying out the new online class schedule for the first time.

According to Associate Registrar Sue Eveland, these comments are typical of the student feedback she's been receiving since the new class schedule debuted March 2.

The most popular feature of the new interactive website is its dynamic searchability. Users can customize their searches in a variety of ways, narrowing the search for courses according to such specifications as availability, time of day, classroom location, number of credits, relevance to General Ed requirements, reduced tuition, or other criteria.

Once a class is selected and the class web page opens, users still have the option to further customize their search or begin another by using the "New Search" menu on the right of the page (see **3** in the illustration above). In the upper right of the page are useful links to the Campus Map and DuckWeb (**2**) , and on the upper left (**1**) you'll find all the course requirements.



*Results of a search for a sociology class using the criteria "Undergraduate," "Reduced Tuition," and "Tuesday-Thursday." Clicking on the class Notes (**4**) takes you to the Course Data page, which includes the Academic Deadlines and an email link to the instructor.*

The new user-friendly website is the product of more than a year of careful forethought and planning. Realizing that students were increasingly bypassing the printed version of the class schedule in favor of the online version (DuckHunt), the Registrar's office began to focus on improving the website.

After months of carefully combing through all the desirable data elements of DuckHunt and Banner and gathering extensive feedback from students, faculty, and administrators, Associate Registrar Sue Eveland and Assistant Registrar Gayle Freeman developed a comprehensive "wish list" of features for the new online class schedule.

Next, they presented the list to Computing Center systems analyst Tim Ketchum with the hope that his programming skills could make their vision a reality. To their delight, Tim not only fulfilled every item on their wish list, he contributed some useful features of his own.

Tim added explanatory mouseovers to course notes, links to web resources for courses that use Blackboard, and direct email links to instructors. He also suggested placing the search menu on each class page for easy access and navigation.

Another major improvement to the class schedule site is that it now updates instantaneously instead of hourly or daily, so that students may be sure they're getting the most up-to-date information.

After trying the new site, most users will probably never return to DuckHunt or the printed class schedule, but to smooth the transition, DuckHunt will remain available into fall term. The last printed schedule of classes will be the winter 2005 schedule.

Our Take on Maxtor OneTouch Backup: Is It Right for You?

Microcomputer Services staff follows up on its promise to test and review the new hard drive backup solution

Dan Albrich
Manager, Microcomputer Services
dalbrich@uoregon.edu

In the Winter 2004 *Computing News*, I discussed a number of backup solutions in the article "Hard Drives: Bigger, Faster, Cheaper…and Less Reliable" (**http://cc.uoregon.edu/cnews/winter2004/hdrives.html**). One of these was the Maxtor OneTouch backup solution, which I promised to test and review in a follow-up article.

To make good on that promise, Microcomputer Services acquired an external Maxtor OneTouch hard disk backup solution and we began our evaluation in February. A summary of our findings is presented below.

General Specifications

We paid $265 for the 200GB version of the drive through **www.cdw.com**. The 200GB and larger versions come with both USB and Firewire ports (important if you need both Windows and Mac compatibility). Lower capacity models with USB-only compatibility are less expensive, presuming you need it only for use with Windows.

System Requirements

Windows: The drive comes with software for Windows 98SE, Me, 2000, and XP.

Macintosh: On the Mac side, both OS 9.1 and higher and OS 10.1.2 and higher are supported.

The drive should work with almost any modern PC. We tested the unit on a Mac running OS 10.3 connected via Firewire, as well as a Windows XP system connected via USB 2.0, without encountering any problems.

While the drive will work with USB 1.0 ports, for performance reasons we strongly recommend you connect only via USB 2.0 or Firewire. Note that Desktop Windows PCs can typically add a USB 2.0 card to the system for less than $75 even when professionally installed. Most Macintosh models already have Firewire ports.

How Well Does it Work?

The product looks like a high quality external hard disk: it comes in a nice looking metal case and the backup button glows blue when the drive is powered on.

Unfortunately, our test drive failed in the first week and we had to return it for a replacement under warranty. The replacement drive seems to be working fine. Given our limited experience with these drives, it's entirely possible we just had some bad luck with the initial unit.

In its simplest form, the drive mounts normally and can be found as a drive letter in Windows, or on the desktop of the modern Mac. Once it's mounted, you can manually drag documents and folders to the disk for backup.

The software bundle works as advertised on both Mac and Windows. The first time you press the button, you're asked to enter some setup information. For example, you need to tell the software which volumes to back up.

After the initial run, subsequent presses on the backup button start the process automatically. By default, the software copies all of the files on your system to the external hard disk except system files or those that are currently in use.

Disaster Recovery

Unfortunately, the backup software included with the OneTouch drive does not make the type of backup that would enable you to restore everything to a new disk transparently. In the event of total disk failure, you would need to manually reinstall system software and any applications you use. The backup disk would still allow you to restore almost any file that was lost in the process. As such, this system is much better than nothing, but it's not as complete as most folks would wish.

To get a "real" backup of the system that takes a true snapshot of your system and restores it exactly the way it was, you'll need disk imaging software—a tool that's not included in the OneTouch software bundle.

Note that while these tools do exist (e.g., Symantec Ghost), they may be difficult or impossible to activate with a specific USB or Firewire external disk due to driver incompatibility. In addition, if the computer's hard disk is formatted for Windows NTFS file format, the Ghost program may not be able to read the data. Most newer PCs use NTFS file systems, so the disk imaging solution isn't as easy to achieve as it may sound.

Hardware issues aside, users must initiate the backup and the computer cannot be used for other purposes while the imaging process completes. The entire process can take more than an hour. Unfortunately, not all users will be patient enough to suspend their activity for that long while the backup process completes—making it more likely that they won't do backups at all.

Our Recommendation

We advise purchasing an external hard disk as part of your backup strategy. This setup has the added advantage of giving you the flexibility to move large data files between home and work.

Whether or not you use the OneTouch system makes little difference. Some folks will prefer manually dragging important files to the external disk, while others will want to have the system do this for them. Either way, an external disk dramatically improves the convenience of backups—making it more likely that you'll actually do them!

CC-Klamath Labs: a Valuable Computing Resource for Individuals and Classes Alike

As the end of winter term neared, these students took advantage of the CC-Klamath drop-in lab to finish assignments.

Have you checked out the computing resources in the CC-Klamath Labs lately?

Tucked away in the basement of Klamath Hall, these labs are often overlooked in favor of their more visible counterparts in the EMU, McKenzie Hall, and Knight Library. But whether you're an instructor needing to reserve lab facilities for classwork, or a student wishing to complete a class assignment, you're likely to find what you're looking for in one of the CC-Klamath labs.

Instructional labs. The two instructional labs, Klamath B13 and B26, have LCD projection equipment as well as whiteboards and wall boards for displaying printed output.

Instructors may reserve lab space by contacting Mary Bradley *(labhelp@uoregon.edu,* **346-1737**). It's generally advisable to reserve instructional labs well in advance of the term needed.

Open-access lab. A large open-access lab adjacent to the instructional labs in B13 and B26 is equipped with the same computers and software as the instructional labs. This arrangement offers an ideal opportunity for classes to take advantage of an instructional facility that can be tightly scheduled, while students who need to use a lab for homework assignments can use the adjoining open-access space during drop-in hours.

The number of available computers and software make the open-access lab a valuable resource for students who need to work on high-end, compute-intensive projects. Student assistants are available to provide technical support during all open hours.

Data storage. Upon request, CC-Klamath staff can provide additional storage for classroom assignments on its servers as space is available. Students can also check out ZIP drives if they'd prefer not to store data on a CD.

Lab Equipment

Open-access lab scanners and printers. Two color scanners and two laserjet printers are available for student use in the CC-Klamath open lab (see hardware list below). Printer fees are payable with UO Campus Cash accounts.To register for Campus Cash On-Line, go to **https://millrace.uoregon.edu/ccash/index.cfm**

Software (all labs):
A wide variety of software and utilities for both PCs and Macs is installed in the labs. In addition to such standbys as Microsoft Office, the software menu includes such specialized tools as ArcView, GIS, and Mathematica, as well as a full complement of multimedia and page layout applications. For a complete list of available software, see **http://darkwing.uoregon.edu/~microlab/cc-klamath_sftw.htm**

Hardware:

- Mac OS G4s w/512MB RAM
- iMacs 1.0Ghz w/512MB RAM w/SuperDrives
- XP-Pro 1.6Ghz Pentium 4s w/ 256MB RAM
- Hewlett Packard LaserJet 4si w/duplex (two-sided) printing
- Hewlett Packard LaserJet4 Plus
- Two color scanners

Lab Hours

During the academic year the lab is open during the following hours:

Mon - Thu	8:00 am - 11:00 pm
Friday	8:00 am - 6:00 pm
Saturday	1:00 pm - 7:00 pm
Sunday	1:00 pm - 9:00 pm

Who's Who at the Computing Center

Meet our new VMS systems manager

Joyce Winslow
jwins@uoregon.edu

Jack Fortune
VMS Systems Manager
Administrative Services and Computing Facilities

A Georgia native with deep roots in the Southeast, Jack Fortune never anticipated moving far from home. But in retrospect, his cross-country trek from Atlanta to Eugene to fill the Computing Center's VMS systems manager slot seems meant to be.

Both Jack and his wife Camilla are ardent outdoor enthusiasts. The couple, both veterans of triathalons, have cycled twice through Southern France, and they also enjoy jogging, hiking, and water sports. Eugene's proximity to biking and running trails, mountains, and waterways make it an ideal locale for the Fortune's favorite pursuits.

In addition, Eugene's midsized, university-town environment was just what the Fortunes were looking for to raise their five-year-old son Julian.

And then there's the VMS manager job: another perfect fit. Jack, who earned an industrial engineering degree from Georgia Tech in 1984, has been working with VMS systems since his senior year in college. He comes to the Computing Center with nearly 20 years' experience in supporting large computer systems. Most recently, he worked at FedEx Trade Networks in Atlanta, where he helped oversee the company's migration from the VAX platform to Alpha and improved system performance, reliability, and availability.

The chain of events that brought Jack and his family to Eugene was serendipitous. Jack wasn't looking for another job, but a posting to a VMS group mailing list caught his eye with a reference to a VMS manager's job opening at the University of Oregon. Jack had always been intrigued by the notion of working in a university environment, where he might be able to make a behind-the-scenes contribution to furthering higher education, so he dusted off his resumé and applied.

Not too long after that, he found himself packing up, putting his house on the market (it sold in a day), saying goodbye to friends and extended family members, and heading west with Camilla and Julian. On February 27, just four days after alighting in Eugene, Jack went to work in his new job at the Computing Center.

Jack's responsibilities at the Computing Center will be much the same as those he's had in the private sector. As a key decision maker shaping the "big picture" of university computing, he will oversee the machines that run the university's administrative programs, helping to configure and adapt them to the university's needs as technology changes and evolves. His first major project will be rolling out the Computing Center's new ABS automated backup system, which is expected to simplify backup processes and improve reliability.

Jack enjoys cycling to work every morning and now that he's had a little more time to settle in, he's getting ready to resume some recreational jogging in his spare time and perhaps even pick up his guitar again. Camilla, who's found a job as a physical therapist at Willamette Community Health Services, is looking for new adventure racing teammates so she can continue pursuing challenging multi-sport events. And Julian is more or less picking up where he left off, attending a Montessori preschool near his new home.

The Fortunes' only regret is having to leave so many family members and friends behind, but they plan to buy a house big enough to accommodate visitors in the near future.

looking for a current map of wireless coverage on campus?

http://geography.uoregon.edu/infographics/wireless/index.html

P2P Applications Can Be Hazardous to Your Computer's Health

Jon Miyake
Acceptable Use Policy Officer
miyake@uoregon.edu

As you know, the Computing Center does not permit P2P (Peer-to-Peer) file sharing applications to be used in ways that infringe on copyright.

Quite aside from the legal ramifications, however, P2P applications have some serious security issues that should discourage you from installing them on your personal computer at home:

1. **P2P applications come with risky third-party software.** Many P2P programs come with third-party applications that are installed as part of the normal installation process. P2P licensing terms explicitly require these programs to be present in order for you to run the P2P application.

   Unfortunately, these third-party programs open the door to pop-up advertising that tracks your computer or web browsing habits, as well as more nefarious security breaches resulting from poor communication or authentication requirements (see the University of Washington white paper on spyware at **http://www.cs.washington.edu/homes/gribble/papers/spyware.pdf** and *NewScientist.com*'s spyware article at **http://www.newscientist.com/news/news.jsp?id=ns99994745**

2. **P2P applications are a vector for viruses.** P2P programs are widely used to distribute viruses. Many of the highly successful viruses in circulation today use P2P programs running on an infected computer as an additional mechanism for propagation.

   In some cases, virus writers may anonymously introduce newly created viruses to the Internet via P2P. In the wild, such newly created viruses are less likely to be detected by your antivirus program.

3. **P2P applications are backdoors for attack.** At least one P2P program has been accused of having a backdoor added to it for unspecified purposes. For more details, see the *afterdawn.com* article, "Backdoor discovered in ES5, the P2P-client," at **http://www.afterdawn.com/news/archive/5004.cfm**

If you're a UO student or staff or faculty member and need assistance removing a P2P application and associated malware (e.g., spyware, adware, viruses) from your computer, please contact Microcomputer Services at **346-4412**.

online resources

Manage Your UO Computing Account Online

Did you know you can simplify some of your everyday account management tasks by performing them online? Here's a handy list of URLs that can make routine tasks such as changing your password quicker and easier.

- Change your password for Oregon, Gladstone, or Darkwing accounts:
  https://password.uoregon.edu/
- Reset your password for Oregon, Gladstone, and Darkwing:
  https://password.uoregon.edu/authorize/
- View your system quota for Oregon, Gladstone, or Darkwing:
  https://password.uoregon.edu/quota/
- Disable or re-enable spam filtering for Darkwing or Gladstone
  https://password.uoregon.edu/allowspam/
- Forward mail from Oregon, Gladstone, or Darkwing
  http://password.uoregon.edu/forward/
- Remove the mail forwarding option from Oregon, Gladstone, or Darkwing
  http://password.uoregon.edu/noforward/

One-stop shopping for account management: You'll also find links to all of these account functions on Microcomputer Services' Account Management web page at **http://micro.uoregon.edu/account/manage.html**

If you have any problems using these online services, please contact Microcomputer Services at *microhelp@lists.uoregon.edu*.

Any questions concerning your account status and other related questions should be directed to the appropriate consultant:

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

Darkwing Faculty/Staff Survey Results:

Susan Hilton
Director, Administrative Services and Computing Facilities
hilton@uoregon.edu

The Computing Center recently conducted a survey of UO faculty, staff, and GTFs regarding their satisfaction with Darkwing and Gladstone, in addition to soliciting input for some possible future directions.

This article is meant to share some preliminary results from that survey based on 460 returned surveys. If you would like to refresh your memory about what we asked, or see the exact wording of a particular question, please see **http://cc.uoregon.edu/ccsurvey.pdf**

Q1. We received responses from 183 faculty members, 214 staff persons, and 51 graduate students. There were 12 surveys with other/no response.

Q2. In response to our question regarding the number of years the person has been at the UO, we saw:

<1 year:	11.4%
1 thru <5 years:	31.0%
5 thru <10 years:	20.7%
10 thru <20 years:	19.6%
20+ years:	17.1%

(totals may not add to 100% due to rounding)

Q3. In terms of self-reported experience/comfort, respondents ranked themselves as:

inexperienced	0.2%
mod experienced	29.4%
quite proficient	57.2%
expert	13.2%

Q4. Users reported they were from:

Administrative units:	27.67%
AAA	4.4%
Business	1.5%
Humanities	7.5%
Journalism	1.1%
Law school	0.5%
Music	2.2%
Natural Sciences	12.8%
Social Sciences	17.5%
Undeclared/other	24.8%

We owe an apology to the School of Education; it was inadvertently left off the list of units as we struggled with our limit of 10 "bubbles" (A-J). We sincerely regret that oversight, and believe many of you from the School of Education contributed to the large "undeclared/other" category.

Q5. We were also curious if there was anyone using both Darkwing and Gladstone: 90% of respondents used only Darkwing; 2.6% used only Gladstone; 4.4% used both; 2.9% used neither.

Q6-20. We then asked about satisfaction with a number of areas. See Figure 1 on the following page for the results.

We will be reviewing this data, as well as written comments you provided (thank you!), to see if there are areas where we can improve our service and performance.

Q21-Q23. We asked respondents to select three possible potential changes. Looking only at the "most important" responses, here's how they voted:

more disk	152 votes
CIFs service	79 votes
easier file restores	58 votes

The fourth-rankedissue appears to be an online calendar. Blogs, compilers, and grids were consistently in the bottom three.

Q24-Q26. We asked if people strongly favored, favored, were neutral, opposed, or strongly opposed three possible procedural changes (Figure 2).

Q27. Finally, we asked you to give us an overall grade. 97.6% of all respondents ranked us satisfactory or better; we appreciate your support and promise to try to do even better in the future!

Excellent	138
Above average	199
Satisfactory	70
Poor	1

Conclusion

Thank you for taking time to complete this survey. We hope you find these results as interesting and useful as we did. If you have any questions or comments, please feel free to contact me at *hilton@uoregon.edu*

How You Voted

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Q6. Email in general:	124	242	31	37	6
Q7. Spam blocking:	133	168	52	65	8
Q8. Virus blocking:	150	174	68	34	6
Q9. Mailing lists:	74	158	87	18	5
Q10. Web pages:	125	227	52	15	2
Q11. Shell access:	54	92	97	13	4
Q12. FTP or SCP:	61	100	78	15	2
Q13. Math/stat software:	11	25	94	8	5
Q14. Streaming media:	10	58	89	20	2
Q15. Consulting support:	85	182	81	27	9
Q16. System availability:	160	232	27	19	3
Q17. System stability:	137	212	39	42	11
Q18. System performance:	103	210	44	67	16
Q19. System capacity:	117	215	49	42	10
Q20. Ability to restore files:	23	92	141	17	11

Figure 1. *Responses to questions 6-20.*

	Strongly Favor	Favor	Neutral	Oppose	Strongly Oppose
Allow users to choose own username:	185	98	99	30	12
Allow multiple usernames:	116	130	129	36	14
Provide forwarding/web site redirection:	200	146	66	11	0

Figure 2. *Responses to questions 24-26.*

Latest Phishing Scams Fake SSL Encryption

The "lock" icon on websites indicating SSL protection is no longer a foolproof safety guarantee now that "phishers" (scammers seeking to trick you into giving them sensitive personal information) are using them deceptively. For details, see

http://slashdot.org/articles/04/03/10/0156200.shtml

http://news.netcraft.com/archives/2004/03/08/ssls_credibility_as_phishing_defense_is_tested.html

http://isc.sans.org/diary.html?date=2004-03-04

Dial 6-0000 for Ernest(ine)

Named after actress Lily Tomlin's acerbic *Laugh-In* TV character, the UO's new voice recognition directory is now at your service

Dave Barta
Manager, Telecom Services
dbarta@uoregon.edu

Too busy to look up a colleague's phone number? Now you don't have to.

Dial 6-0000 from any campus phone and a slightly stuffy voice we call Ernest(ine) will ask you to state the name of the university employee you're calling. When you do, the UO's new Ernest(ine) voice recognition directory will interpret your request and transfer the call.

The new directory performs this task correctly approximately 95 percent of the time. If it doesn't understand you, it will offer some reasonable options (for example, if you've asked for a name that matches more than one UO employee, Ernest(ine) will list all the matching names together with their departments and ask you to pick the right one).

Ernest(ine) is a speech recognition system manufactured by Phonetic Systems which UO Telecom Services installed over the last few months with help from Computing Center programming staff. It is one more piece of an evolving suite of integrated campus directory systems that also includes the printed telephone directory, the online web directory, and the operator lookup system. All of these systems make use of the Computing Center's new LDAP Directory Service, which obtains data from the Banner HRIS database.

To increase its accuracy, Ernest(ine) creates logs of lookups that don't work and includes a database of nicknames and unusual pronunciations. (If you find that Ernest(ine) is mispronouncing your name, press * after Ernest(ine) has initially answered your call and the system will help you create a **.wav** file with the correct pronunciation. Or, call Eric Fullar at **346-5966** for assistance.)

At this point, Ernest(ine) includes listings only for departments that appear in boldfaced type in the printed directory. This database is currently being restructured to include a hierarchy of department listings and sublistings, as well as cross references and an assortment of other information compiled over the years by retired Operations supervisor Dorothy Grover. Also in the works is the installation of a new telephone number which you can call to obtain faculty and staff email addresses.

In addition to the 6-0000 number, you can reach Ernest(ine) outside normal operator services hours at the regular operator 6-1000 number. Eventually, Ernest(ine) will be the first point of contact at that number at all hours, backed up by live operators during regular working hours.

Thanks to Associate Professor Steven Hecker of the Labor Education and Research Center for his inspired choice of "Ernest(ine)" as the name of the new directory system!

Sometimes Being Very Small Can Be Very Big:

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

While attending Innotech Oregon 2004 at the Oregon Convention Center in Portland last month, I had a chance to sit in on two sessions relating to ONAMI. If, like me, you didn't know ONAMI existed, read on. ONAMI is, and will continue to be, tremendously important for the UO, Oregon, and the United States.

What Is ONAMI?

ONAMI (literally, "great wave") is the Oregon Nanoscience and Microtechnologies Institute, a collaborative project undertaken by the University of Oregon, Oregon State University, Portland State University, and the Pacific Northwest National Labs (PNNL), in conjunction with industry partners and others. ONAMI focuses on research at the micro and nano scale, and is designed to position Oregon as a national leader in nanotechnology research and development. You can visit the ONAMI web site at **http://www.onami.us/**

Why Is Nanotechnology Such a Big Deal?

A conservative rule to use when evaluating new projects is to look at their funding and the people they attract. In the case of nanotechnology in general and ONAMI in particular, both the funding and the personnel are impressive: from the President of the United States on down, nanotechnology has attracted important interest and support.

On December 3, 2003, President Bush signed the "21st Century Nanotechnology Research and Development Act," which was co-authored by Oregon's very own Senator Ron Wyden. That act appropriated $3.7 billion (with a "b") dollars over four years for nanotechnology-related programs. For the full text of the act, see **http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ153.108**

Oregon's legislature and Governor Theodore Kulongoski are likewise very supportive, having appropriated $21 million in bonds to help subsidize ONAMI. According to an *EE Times* report (**http://www.eetimes.com/at/news/showArticle.jhtml?articleID=18700587), t**otal funding for ONAMI is about $75 million. Governor Kulongoski also personally appeared to give a speech at Innotech, signalling both his personal interest in nanotechnology and his confidence in ONAMI.

At Innotech, the vice presidents for research at UO, OSU, and Portland State shared information about nanotech-related programs at their respective campuses, as did senior technical managers from PNNL, HP, Intel, and other organizations.

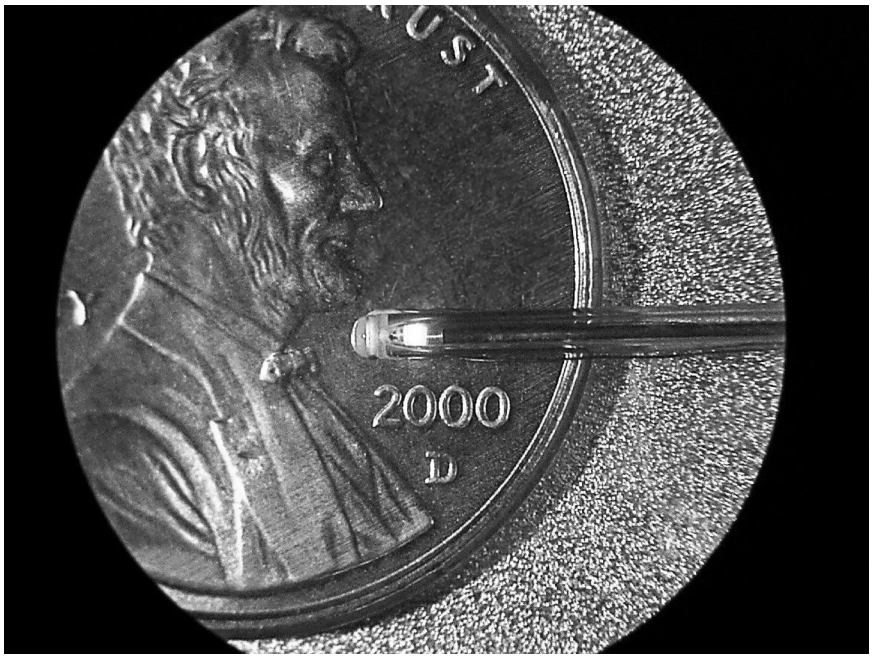


Photo: Richard Peterson, OSU

In a graphic demonstration of nanoscale, a nanocombuster is shown in relation to a penny. The tip of the combuster is glowing just above the year "2000" engraved on the penny.

It is hard to get much bigger names, or much greater financial support, for any project these days. But let's not get tied up in politics and financial issues!

Just How Small Is A Nanometer?

Nanometers are ***very*** small.

Mechanically speaking, a nanometer is 1x10^-9 meters (e.g., there are a billion nanometers in one meter).

Most of us have a hard time conceptualizing abstract measurements that small. To help people visualize the minute scale of a nanometer, the most commonly used example is a strand of hair: a single human hair is normally 60,000 to 120,000 nanometers wide!

A nice graphic representation of things at the microscale and nanoscale can be found at **http://www.sc.doe.gov/bes/Scale_of_Things_07OCT03.pdf**

ONAMI and Nanotechnology

Who Are the Leading Competitors?

Perhaps the leading competitors in nanotechnology are the six universities that have already been designated as NSF Nanoscale Science and Engineering Centers, charged with work in a particular area of applied nanotechnology. Those six schools are Columbia, Cornell, Harvard, Northwestern, Rensellaer Polytechnic Institute, and Rice. UCLA has also been tapped to lead a nano manufacturing center, as has the University of Illinois Urbana Champaign. For more information on these nanotech centers, see

http://www.nsf.gov/home/crssprgm/nano/centers.htm

Outside of Oregon, other schools that are also working in the nanotechnology area include Northeastern, Notre Dame, Purdue, and South Carolina.

This is an incredibly important area, and one where Oregon is committed to meeting the competitive challenge.

What Does Nanotechnology Have to Do With Computing?

The intimate connection between nanotechnology and the future of computing is perhaps best illustrated by Intel's deployment of a production 90nm semiconductor manufacturing facility in Hillsboro (see **http://www.intel.com/pressroom/archive/releases/20020813tech.htm**), and their demonstration of 65 nm SRAM chips (see **http://www.intel.com/pressroom/archive/releases/20031124tech.htm**).

Nanotechnology will be intimately tied to virtually all the most advanced processors and related technology you'll be seeing in the years ahead.

Where Can I Find More Information?

Below is a list of online resources pertaining to Innotech, ONAMI, and nanotechnology:

1. Innotech 2004
   http://www.innotechor.com/
1. ONAMI
   http://www.onami.us/
2. NSF Nanoscale Science and Engineering
   http://www.nsf.gov/home/crssprgm/nano/
3. National Nanotechnology Initiative:
   http://www.nano.gov/
4. Scientific American Nanotechnology Coverage
   http://www.sciam.com/nanotech/
5. Nanotechnology (Yahoo Directory)
   http://dir.yahoo.com/Science/Nanotechnology/
6. Nanotechnology (Open Directory)
   http://www.dmoz.org/Science/Technology/Nanotechnology/

A Glimpse of ONAMI Research Activities on Campus:

Contact angle goniometry: *Using a device donated by Intel Corporation, UO chemistry Ph.D. student Jenny Dahl employs a classic technique for looking at nanoscale films on surfaces.*

Electron beam lithography: *UO researchers Nick Liebrecht (foreground) and Kurt Langworthy etch a 20-nanometer pattern on silicon to make nanoelectronic devices using equipment in the UO's MicroAnalytical Facility.*

A Closer Look at Subversion: the Latest

This new version control system is a good general purpose tool for tracking changes to files

Anthony Kay
Student Consultant
User Services and Network Applications

Subversion is a relatively new version control system that is meant to be an improvement on the widely used Concurrent Versions System (CVS). Both of these tools are intended to allow multiple developers to check out working copies of source code so that concurrent development can occur on different sections of an application or document.

I have been using Subversion for over a year now, and have found it to be useful in any situation where I want to keep track of changes to files. Specifically, I use it in the following situations:

- managing the source code of software I am developing
- keeping track of my day-to-day files and documents, including images and other binary files
- distributing versioned files to users who have only a web browser
- tracking configuration files as a UNIX administrator

Subversion or CVS?

Subversion is a new project, and CVS has been around a while and is widely used. So what are the reasons to use Subversion?

- Subversion tracks directories and renames and copies files. CVS does not.
- Subversion's network support is done through Apache and a Subversion module. This gives you the ability to manage access control with Apache, and adds the ability to browse the repository with a web browser for free. CVS has network support, but it is not easily extensible or interoperable.
- Binary files are well supported in Subversion, and MIME types can be easily associated with files. CVS does not deal with binary files very well. This means you can reliably store images and other binary files in Subversion.
- Subversion's techniques for branching and merging are greatly simplified over those in CVS.

Alternatives to CVS and Subversion

The world is never one-size-fits-all. There are many ways to keep track of changes to files. One way is to do daily backups and keep them for a couple of years. I would argue that this particular choice is inferior in most respects: almost no one is willing to bother with backups every day, and finding the right backup that contains the file you want can be a real chore.

Subversion is meant to be a general purpose tool. It keeps track of files and changes to those files. If you are looking for it to do more, then it might be a good idea to check for tools that are more specialized for your needs. A popular choice for web developers is to use a content management system like OpenCMS (**http://www.opencms.org**), which not only versions your files, but is tuned for web page development. The disadvantage of specialized tools is that they may be less adept at version control, may be more resource intensive, and may be more complex to install and configure.

So How Does It Work?

The basic idea is that there is a central repository that keeps track of a group of files, including every change that is made to them. Individual developers check out a copy of these files, make changes to their private copy, and when they have something useful to submit they commit their changes back to the central store. Changes made by one developer cannot be seen by anyone else until they're committed.

Committed changes can be pulled into someone's working copy at any time. This allows individual developers to merge the changes made by others into their own working copy so they can track the progress of the project as a whole.

Of course, there is nothing that says you have to use Subversion with more than one developer. I use it all the time for things that are unique to my environment. For example, I store most of my UNIX home directory in Subversion. This allows me to keep tabs on all of my important files, and even allows me to share all or part of my home directory among my machines, such as my desktop and laptop. When I make a change to a file, I commit the changes to the central repository and it is then available for checkout on my other machines.

Storing these files in a versioned system also gives me the ability to recover files deleted long ago, undo changes to configurations that have proved to be unworkable, or restore files that I've accidentally erased. Another plus is that when I make a backup of my Subversion repositories, I am also backing up a complete history of my important files. Finally, the fact that I keep a working copy checked out on multiple machines means that I am well-protected from data loss due to catastrophe or theft. I could lose all of my backup CDs and my repository machine in a fire, but if one of the machines that has a working copy survives, then I at least have a pretty recent version of my files intact.

On the down side, using Subversion will increase your disk space usage by quite a bit. This is usually not a concern on personal machines, where people usually have space to spare, but it may be a concern if you have a disk quota on a multi-user machine. The repository itself will be at least as big as your initial set of files, and it will grow; each working copy, which includes the files you are to work on as well as a hidden copy of those files

in an unmodified state, usually takes more than three times the disk space as an unmanaged set of files.

As an example, my open-source projects directory contains about 3MB of source files when exported from Subversion (i.e., as unmanaged files). The working copy for these same files takes 11MB. The repository that keeps track of them is currently at revision number 196, and takes 6MB.

The small size for the repository may seem a bit odd at first, especially since it has the complete history of 196 different versions of my files! This paradox is resolved by the fact that the repository only has to track the differences in the files from one version to the next. For example, in revision 192 I may have changed only one line of one file. That one line and the context for it (i.e., file and location) are all that has to be stored in order to move from version 192 to 193.

Space usage can be mitigated somewhat if you run the repository on a personal machine,and keep only a working copy on the multi-user machine. This is in fact what I do with my UO computing account, where a good portion of my home directory is really a working copy that has been checked out of a Subversion repository that is running on my own networked Linux box.

Installing Subversion

This step can be very easy or very difficult depending on your target OS and personal level of control over the hardware. Subversion can be built as a user of any of the supported operating systems, but the easiest way to install it is to use precompiled packages, which require that you have unlimited access to the configuration of your target system. If you are trying to build it yourself, then be prepared to spend some time getting it all correct.

The simplest platforms on which to use Subversion are the ones that have binary distributions: Linux, Mac OS X, and Windows. A GUI client called RapidSVN is also available. It uses the wxWindows toolkit to give it some platform independence, and there are binary versions for Windows and a few variants of Linux.

If you are using Windows, you can also download a GUI system called TortoiseSVN, which integrates with Windows Explorer to give you point-and-click access to your file management functions.

Setting up a repository

The first thing to do in order to use Subversion is to create a repository. This is nothing more than a directory that stores the Subversion database for a set of files. You can have as many repositories as you want, and I suggest making different repositories for files that need different levels of security. For example, I do not want to share my UNIX home directory with the world, so I put that in a repository that has very strong access restrictions (SSL and authentication required). I also work on projects that I make freely available on the Internet. I make those repositories read-only, and require authentication for committing changes.

The creation steps are the same for either kind of repository. The physical separation just gives you a way to easily break up your security policies later. To create a repository, type the command:

```
svnadmin create name
```

Where *name* is the name of the directory into which your new repository should be created. The directory should not already exist, but the path to it should. Once it is created, you should change the ownership and permissions on the directory to appropriate settings. For example, if the repository will only be used through Apache, then the person who runs Apache should be the owner of the repository. The repository owner should also be the only one who can read/write the repository files.

If you are using a binary distribution of Subversion, then you should have gotten a precompiled version of Apache and the modules needed to run a networked Subversion repository. The security of a network repository is completely controlled through Apache, and the instructions for setting up simple network access can be found in the Subversion Book available from **http://subversion.tigris.org/**

Networked vs. local access: I find that the networked method of access is better in the long run for almost all uses, because it avoids permission, ownership, and process interruption issues that can cause problems with direct disk access. Nevertheless, some users may need to use local disk instead of networked access. I have two warnings for those users:

1. Do not try to interrupt Subversion commands. Killing the commands can leave locks in bad states. I have never lost data because of this, but I have had to go into the repository database directory and run **db_recover** to fix stale locks, or **svn cleanup** to do the same for a working copy.
2. You will have problems if you want to work with multiple read/write users. The transaction logs are created with owner-only permissions, so even being in the same group doesn't help. There may be a workaround, but I am not aware of it. Note that if you are the only one who will write, then there is no problem.

Where to Find Examples

An expanded HTML version of this article with detailed examples of how to manage files with Subversion is available at **http://darkwing.uoregon.edu/~tkay/subversion.html**

References

1. Subversion Home Page: **http://subversion.tigris.org/**
2. Apache Web Server Installation and Configuration: **http://www.apache.org/**

"How *Did* They Get My Email Address?"

Online marketers and 'e-pending:' Why witholding your email address may not keep marketers from emailing you

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

In some cases, you may do business with a company but not provide them with your email address. Nonetheless, you may suddenly be surprised to find that that company is contacting you by email! How *did* they get your email address if you didn't give it to them?

In a word: "e-pending," or email address appending.

E-pending is the process of "augmenting" an existing customer record with the customer's email address or other information—information which has been obtained (for a fee) from some other party. Numerous commercial entities offer this as an online "service," in some cases relying on nebulously obtained "opt-in" email addresses.

Obviously this can raise significant privacy issues (particularly in cases where the e-pending may have been done inaccurately, potentially resulting in confidential customer information being sent to the wrong person, or customers failing to receive notices that they wanted and otherwise would have received via a postal mail address that they'd provided, or other channels).

For your own privacy and security, we recommend that you avoid transactions with companies known to engage in e-pending.

If you yourself are contemplating e-pending email addresses to a database you maintain, we strongly recommend against it.

References

Note: *The references provided below are listed for your edification only, and their mention should not be construed as endorsement of the policies or practices they espouse.*

1. Direct Marketing Association's new guidelines for the use of e-pending by its members:
http://www.the-dma.org/cgi/disppressrelease?article=552
2. AIM/CRE Recommendations for E-mail Append
http://www.interactivehq.org/councils/CRE/bpappend.asp

What's New in the Documents Room?

Vickie Nelson
Documents Room Librarian
vmn@uoregon.edu

The Computing Center Documents Room is constantly adding new items to its collection. The following titles are among our most recent acquisitions. To explore our collection further, visit us on the web at **http://darkwing.uoregon.edu/~docsrm/** or in person at 175 McKenzie. Our hours are 9:30 A.M. to 5 P.M., Monday through Friday. Call **346-4406** for more information.

Before & After Page Design by John McWade
The founder and publisher of *Before & After* magazine uses a series of projects from the pages of his magazine to illustrate design principles that will help desktop publishers communicate more effectively.

Defensive Design for the Web: How to Improve Error Messages, Help, Forms, and Other Crisis Points
by Matthew Linderman and Jason Fried
The authors, members of the web design and usability specialists "37signals," offer vital tips to web designers.

Degunking Windows
by Joli Ballew and Jeff Duntemann
A good maintenance manual for non-expert windows users who want to improve their computer's performance.

DNS on Windows Server 2003
by Robbie Allen, Matt Larson, and Cricket Liu
This updated O'Reilly book covers what administrators need to know to manage DNS, including system tuning, caching, and zone change notification.

Exploiting Software: How to Break Code
by Greg Hoglund and Gary McGraw
For security professionals who have to be better than the bad guys in finding and exploiting holes in software.

The Extreme Searcher's Internet Handbook: A Guide for the Serious Searcher
by Randolph Hock and Gary Price
Loaded with tips and tricks to help you hone your searching skills, this book also includes sections on citing Internet sources, uncovering the so-called invisible web, and the basics of copyright.

The Little Mac iApps Book
by John Tollet and Robin Williams
For users eager to get started with the slew of applications that came with their new Macintosh. Covers iTunes, iDVD, iMovie, iPhoto, iCal, Mail, Safari, and Mac.com.

Typographic Principles (CD-ROM)
by Linda Weinman and Don Barnett
This CD provides 90 minutes of instruction on the fine points of designing with type.

« cybercrime in the news »

More on Nigerian 419 Scammers…

'Operation Tidal Wave.' In December, an intercept by British customs agents led to the arrest of a principal actor in a counterfeit check scheme that is the latest mutation of Nigerian "419" fraud (an email scam named after the section of Nigerian penal code it violates). This particular scam targets individuals who are trying to sell something on Internet auction sites such as eBay. The arrest was part of "Operation Tidal Wave," an international crackdown on Nigerian Internet fraud. For details, see

- "Man indicted in Nigerian scam"
  http://www.post-gazette.com/pg/04037/269905.stm
- "Nigerians running lucrative swindles; Trail leads to man in North Versailles"
  http://www.post-gazette.com/localnews/20040118scammerlocal5p5.asp

Trial of alleged bank swindlers opens in Nigeria.

Five Nigerians accused of swindling a Brazilian bank out of $242 million are now on trial in their home country. The discovery of this scam has resulted in criminal investigations in Switzerland, Britain, the U.S., and Brazil. For details, see
http://news.bbc.co.uk/go/pr/fr/-/2/hi/africa/3460861.stm

Alleged big-time Nigerian scammer nabbed. An Australian man accused of heading a global multi-million dollar scam using a variation of the classic Nigerian 419 swindle that lures the greedy and the gullible with empty promises of big rewards. This particular scam stole up to $5 million from people in more than 10 countries, more than half a million of it from a Saudi sheik. See
http://australianit.news.com.au/articles/0,7204,8146011%5E15330%5E%5Enbv%5E15306-15319,00.html

"Buffalo Spammer" Rapidly Convicted

After a four-day trial, "Buffalo Spammer" Howard Carmack was convicted of forgery, falsifying business records, and identity theft in connection with his spamming operation. Carmack could get up to seven years in prison, and prosecutors hope other would-be spammers will take note. For details on the case, see
http://www.newsday.com/news/local/wire/ny-bc-ny--buffalospammer0331mar31,0,1490329.story

http://www.buffalonews.com/editorial/20040325/1052573.asp

Crackdowns on Child Porn Websites

In January, federal authorities charged nearly two dozen people in New Jersey and 20 others around the nation with downloading child pornography from Regpay Co. Ltd, an Internet processor of website subscriptions in Minsk, Belarus. Regpay and Connections USA, of Fort Lauderdale, Florida, were also charged in the scheme.

In another legal action, a Florida man who directed children to pornographic websites using a domain-name scam was imprisoned for two and a half years in February. For details, see

- "Credit card firm at center of child porn ring"
  http://www.cnn.com/2004/LAW/01/15/child.porn.arrests.ap/index.html
- "US porn typosquatter banged up"
  http://www.theregister.co.uk/content/6/35901.html
- "Notorious URL Scammer Pleads Guilty"
  http://dc.internet.com/news/article.php/3287981

Convicted Spammers Get Stiff Jail Time

A pair of co-conspirators in a fraudulent email advertising operation that gleaned thousands of stolen credit card numbers were recently sentenced in federal court. The chief perpetrator Helen Carr was sentenced to 46 months and her accomplice, to 37 months.
http://home.hamptonroads.com/stories/story.cfm?story=64935&ran=83091

Romania Tackles Cybercrime Wave

In recent years, Romania has taken the lead in international Internet auction fraud schemes, and authorities there are trying to reverse the trend, with some success. See
http://news.bbc.co.uk/2/hi/technology/3344721.stm

Adobe Cooperates to Thwart Counterfeiters

Earlier this year, Adobe Systems Inc. acknowledged that it had added some counterfeit-busting features to its popular graphics software at the request of government regulators seeking to protect the integrity of the world's major currencies. For details, see
http://www.eweek.com/article2/0,1759,1430991,00.asp

'Hackmailers' Under Investigation

Extortion gangs threatening online betting businesses with denial of service attacks are being tracked down by the UK's National Hi-Tech Crime Unit, which claims it's closing in on the perpetrators.
http://www.silicon.com/software/security/0,39024655,39118977,00.htm

WebTV Hacker Charged with Cyberterrorism

An alleged malware scripter who tricked a small number of MSN TV users into running a malicious email attachment was arrested and charged with cyberterrorism under the provisions of the US PATRIOT Act. The malicious script reprogrammed the TV set-top boxes to dial 9-1-1 emergency response
http://www.securityfocus.com/news/8136

Australian Domain Name Scam Busted

Con artists trading in bogus domain names were intercepted before they could skim more than half a million dollars from unsuspecting victims. See **http://www.nzherald.co.nz/business/businessstorydisplay.cfm?storyID=3560128&thesection=business&thesubsection=technology&thesecondsubsection=information**

The Art of Computer Security: How You Can Protect Your Little Corner

Jon Miyake
Acceptable Use Policy Officer
miyake@uoregon.edu

The web of computer security is composed of firewalls, policies, filters, system scans, grumpy system administrators, overworked technical support people, patches, updates, antivirus programs, anti-spyware programs—and finally *you*, the beleaguered user.

Even when all these components work together like a well-oiled machine, complete computer security is not assured. However, if everything's running smoothly, the likelihood of your machine becoming compromised is relatively low. By making your little corner of the network secure, you increase overall network security for the rest of campus and the rest of the Internet.

Make Use of the UO's Security Resources

UO systems administrators do their part to protect the campus network by filtering problematic Internet traffic at the UO border, requiring secure passwords and enforcing the use of secure protocols and applications, scanning the network, and "defanging" or filtering email attachments on Gladstone, Darkwing, and Oregon.

The UO also provides several resources to assist you in keeping your computer secure:

1. a site-licensed antivirus program (Norton AntiVirus)
2. a UO Security CD (available in 151 McKenzie Hall)
3. Virtual Private Network (VPN) support for off-campus users
4. an online test to detect critical Microsoft security flaws (MS03-026, MS03-039, and MS 04-007) on your PC (**http://pctest.uoregon.edu/**)
5. the Computing Center's newsletter, *Computing News*
6. Microcomputer Services' security self-help site (**http://micro.uoregon.edu/security/**)
7. contacts for reporting UOnet-related abuse (**http://cc.uoregon.edu/abuse.html**)
8. technical discussion lists such as uosecurity and deptcomp; to subscribe, see **http://lists.uoregon.edu/listjoining.html**
9. technical support (*microhelp@lists.uoregon.edu*)
10. the UO security group (*security@uoregon.edu*)

Other Things You Can Do

Here are some additional things you can do to keep your computer secure:

1. **If automatic updates are available for your operating system and applications, use them.**
2. **Periodically check your software vendors' websites for updates to ensure that your system is being patched.**
3. **Reboot your computer regularly to ensure that patches take effect**. You may already be doing this if you turn off your computer when you go home at night and turn it back on upon returning to work the following day. If you're not in the habit of turning your computer off daily, reboot once or twice a week to ensure that new patches are fully applied. Rebooting also keeps your computer happy by clearing cruft (electronic garbage) out of memory.
4. **Even if you have a brand-new computer, get a copy of the UO Security CD from 151 McKenzie Hall and run it *prior* to connecting it to the network.**

   As we learned during the July 2004 Blaster and Nachi virus outbreaks, not-yet-secured computers can be infected within *10 seconds* after being connected to the network!
5. **Use an antivirus program and keep it up-to-date.** Your computer may have come with an antivirus product when you purchased it. Unless you specifically paid extra for it, this product is essentially a demo version and usually expires within three months after activation.

   For an antivirus program to be effective, it needs to be completely current. We recommend that you remove the antivirus program that came with your system and install Symantec's Norton AntiVirus, which is site-licensed at the UO (see **http://micro.uoregon.edu/av/nav.html**). This license permits you to access updated virus definitions—a critical feature when three or more new viruses are discovered almost every day.

   Once Norton AntiVirus is installed, activate its AutoProtect feature, periodically run LiveUpdate, and schedule routine scans of your computer.

of the Network

If you're not running a Microsoft operating system… Don't allow yourself to be lulled into a false sense of security just because you're not running a Microsoft operating system. Virus authors are perfectly capable of targeting other platforms—and will, as soon as these platforms become popular. No matter what operating system you're running, you need to keep it up-to-date and secure.

6. **Use an anti-spyware product such as Spybot (http://www.safer-networking.org/), or Ad-aware (http://www.lavasoftusa.com/software/adaware/).**

7. **Run a firewall product.** At the very least, enable the firewall that comes with your operating system (e.g., Windows' ICF, Mac OS X's IPFW, Linux's IPTables/IP Chains).

   In addition, consider using a software firewall product (e.g., *BlackIce*, *Symantec Internet Firewall*, *ZoneAlarm*) if you are involved in high-risk activities such as running P2P applications (Gnutella, Kazaa, eDonkey, Bittorrent, and the like), downloading programs or games from the Internet, or using Internet Explorer, Outlook, or Outlook Express.

8. **Don't click on or otherwise execute attachments that you are not expecting—even if they are from someone you know.** There is no absolutely foolproof way of verifying that the attachments are benign.

9. **Avoid Internet Explorer, Outlook, or Outlook Express.** Although feature-rich, these programs have a track record of being viral vectors and/or enablers.

   Microcomputer Services or your local technical support staff should be able to recommended alternatives that will meet your requirements. Some viable alternatives for Outlook/Outlook Express are Bat, Pine, Mulberry, and Eudora. Alternatives for Internet Explorer include Netscape, Mozilla, Firefox, and Opera.

   If for some reason you absolutely must continue using IE, Outlook, or Outlook Express, please make sure you run Office and Windows updates frequently.

   If you need further information about the security risks associated with these Microsoft applications, contact Microcomputer Services (*microhelp@lists.uoregon.edu*) or the UO Security Group (*security@uoregon.edu*).

'I Think I Have a Virus… What Should I Do?'

If you suspect your computer is infected, the action you take will vary somewhat depending upon your particular scenario, as described below:

1. 'My antivirus program discovered it!' If your antivirus software identifies a malicious program and quarantines, deletes, or fixes it, you should do a little research about the virus. Find out what it does, how it propagates, and how long it may have been on your computer. If necessary, contact your local computer support professional, Microcomputer Services (*microhelp@lists.uoregon.edu*), or the UO Security Group (*security@uoregon.edu*) for advice on preventing reinfection.

If your antivirus program identifies an infected file but does *not* quarantine, delete, or fix it, reboot your system in safe mode and do a full system scan for viruses. This can be a common problem with Windows NT, 2000, and XP systems.

2. '**Network Security discovered it!'** Unless you're capable of removing the virus yourself, turn your computer off until technical support can assist you.

We *strongly* recommended not using a machine that is virally infected. The longer a virus is on the system, the more damage it can do to your files. There has been an increase in extremely malicious viruses that will delete or modify files on compromised systems. These types of viruses not only cause problems for you, but due to their potential access to network shares they can also modify, delete, and infect files belonging to your co-workers.

3. 'Someone I know told me my computer is virally infected.' To be on the safe side, verify that your computer definitions are up-to-date and run a full system scan. It could be that a virus is forging ("spoofing") your email address account in infected email. In such cases you will see rejected email that you did not send arriving in your Inbox with a notice that your message had a viral attachment or was otherwise undeliverable.

4. 'I have Norton AntiVirus installed but it doesn't work.' This is often a really bad sign. *Immediately contact your local technical support or Microcomputer Services for assistance.*

5. 'My computer has gone wonky.' Your system instability could be due to a variety of factors, including infrequent rebooting, failing or conflicting hardware, corrupted files, insufficient memory—or last but not least, a viral infection. Contact your local technical support or Microcomputer Services for advice.

Security Alerts…

— Microsoft —

Microsoft Releases Fixes for Twenty New Windows Flaws in April

On April 13, Microsoft released patches for flaws affecting Windows, Internet Explorer, and Outlook Express. Some of these could make the operating system vulnerable to new worms or viruses similar to the highly destructive MSBlast worm, which has infected at least eight million Windows computers since last August. For details, see

- "Microsoft Windows Security Bulletin Summary for April, 2004"
  http://www.microsoft.com/technet/security/bulletin/winapr04.mspx
- "MSBlast epidemic far larger than believed"
  http://news.comcom/2100-7349-5184439.html
- "Microsoft warns of a score of security holes"
  http://zdnet.com.com/2100-1105-5190818.html

Critical Microsoft Windows Flaw Requires Immediate Patch

A flaw in Windows' ASN.1 Library could allow malicious code execution. Affected software includes:

- NT Workstation 4.0 Service Pack 6a, NT Server 4.0 Service Pack 6a
- Windows 2000 Service Packs 2, 3, and 4
- XP and XP Service Pack 1
- XP 64-bit Edition & XP 64-bit Edition Service Pack 1
- XP 64-bit Edition 2003 & XP 64-bit Edition 2003 Service Pack 1
- Windows Server 2003 & Windows Server 2003 64-bit Edition

For more details, including some important caveats, see **Microsoft Security Bulletin MS04-007** ("ASN.1 Vulnerability Could Allow Code Execution…") at **http://www.microsoft.com/technet/security/bulletin/ms04-007.mspx**

UO Windows users: Test your PC for the MS04-007 vulnerability, as well as MS03-026 and MS03-029, by using the "Test My Computer" link at **http://pctest.uoregon.edu/** The latest version of the free **Windows Security CD** distributed by Microcomputer Services (151 McKenzie) contains the patches for all of these critical flaws.

Flaw Detected in Virtual PC for Mac

An "important" flaw that could be exploited by malicious code was detected in Virtual PC for Mac early this year. Versions 6.0, 6.01, 6.02, and 6.1 are affected. For details, see **Microsoft Security Bulletin MS04-005** ("Vulnerability in PC for Mac could lead to privilege elevation…") at **http://www.microsoft.com/technet/security/bulletin/ms04-005.mspx**

Get Patches for Outlook, MSN, Windows Media Services

Early in March, Microsoft warned of vulnerabilities in three of its top products (Outlook 2002, Windows Media Services, and MSN Messenger 6.0 and 6.1).

Outlook. Of the three, Outlook 2002's vulnerability is considered the most dangerous, as it could ultimately allow attackers to gain control of a user's computer and run malicious code. You can get the Outlook 2002 Security Patch KB828040, along with downloading instructions, at **http://support.microsoft.com/?kbid=828040**

MSN. This flaw could allow attackers to view the contents of a victim's hard drive during a chat session, especially if anonymous callers are not blocked. More information is available on Symantec's security response site at **http://securityresponse.symantec.com/avcenter/security/Content/9828.html** For patches and downloading information, see **MS04-010** at **http://www.microsoft.com/technet/security/bulletin/ms04-010.mspx**

Media Services. A flaw in the way Windows Media Services software handles TCP/IP connections could allow a denial-of-service attack on the server. See Symantec's security response site at **http://securityresponse.symantec.com/avcenter/security/Content/9825.html** for details. The patch is available at **http://www.microsoft.com/downloads/details.aspx?FamilyId=7F4C067C-5D34-48FB-A9FA-C2200243D4D2&displaylang=en**

Windows Code Leak Exposes Potential Critical IE 5 Exploit

On February 12, Microsoft confirmed that portions of the source code for Windows NT 4.0 and 2000—including code for Internet Explorer 5—had been illegally posted on the Internet.

Security researchers subsequently found and tested a flaw that exists in all versions of IE 5 for *all* Windows versions as a result of the code leak. Microsoft advises IE users to upgrade to IE 6 immediately.

For details, see

- "Leaked Windows Code Opens IE Hole"
  http://www.pcworld.com/news/article/0,aid,114816,00.asp
- "Microsoft Confirms Windows Code Leak"
  http://www.washingtonpost.com/wp-dyn/articles/A37648-2004Feb12.html

Serious New IE Spoofing Problem

Internet Explorer users are vulnerable to a flaw that allows a malicious user to create a hyperlink to a counterfeit website. The bogus site appears benign and legitimate in every way, thus easily fooling visitors into downloading files that harbor computer viruses. Information on how to protect yourself from this scam, known as "spoofing," is available at **http://support.microsoft.com/default.aspx?scid=kb;en-us;833786** Also see **Security Bulletin MS04-004**, "Cumulative Security Update for Internet

Explorer," which replaces MS03-048, at **http://www.microsoft.com/technet/security/bulletin/ms04-004.mspx**

Free Microsoft Security CD Available

In February, Microsoft launched a *Windows Security CD* giveaway program for users of Windows XP, Me, 200,98, and 98 SE (Second Edition). The CD contains all MS "critical" patches through October 2003, as well as free antivirus and firewall trial software. It is intended to reach users whose slower Internet connections prohibit them from being able to download patches over the network. To order the free CD, go to **http://www.microsoft.com/security/protect/cd/order.asp**

Windows Patches Targeted by Hackers

The BBC News Online reported recently that malicious hackers are waiting for Microsoft to identify loopholes and issue patches before devising their attacks. The report said that often the patch itself was the catalyst for exploiting a particular vulnerability, indicating the need for users to patch security loopholes as soon as possible. For details, see "Hackers exploit Windows patches" at **http://news.bbc.co.uk/1/hi/technology/3485972.stm**

— Worms —

Beagle/Bagle Virus (affects Windows 2000/95/98/Me/NT/XP)

In late January, a series of mass-mailing worms variously known as W32.Beagle or Bagle began circulating on the Internet. As of March 22, there were more than a dozen known variants of the worm, which arrive via email and create a security hole ("backdoor") through which they can penetrate a victim's machine.

Beagle.F and Beagle.G also attempt to spread across filesharing networks such as Kazaa and iMesh. Beagle.Q infects its victims *without* requiring them to open an attachment. All variants use "spoofed" or forged **From:** email addresses. Beagle worm attachments have the suffix **.zip** (Beagle.G uses password-protected zip files in an effort to break auto-unzipping virus scanners).

The Beagle.J variant that hit campus on March 2 fooled many UO users because it purported to be an official security warning from campus authorities. *Microcomputer Services has published information on protecting yourself against the Beagle.J worm and other variants on its security website at* **http://micro.uoregon.edu/av/beagleJ.html**

W32/Netsky.R@mm (affects Windows 2000/95/98/Me/NT/XP and Windows Server 2003)

Another mass-mailing worm that began circulating in February, and, like Beagle, propagates via **.zip** files and may also spread through filesharing networks. For more information, see **http://www.symantec.com/avcenter/venc/data/w32.netsky.r@mm.html**

MyDoom/W32.Novarg.A@mm (affects Windows 2000/95/98/Me/NT/XP)

Using similar tactics as Beagle and Netsky, and masquerading as an email error, this worm rapidly spread worldwide in January, causing billions in economic damage in 215 countries. See **http://securityresponse.symantec.com/avcenter/venc/data/w32.novarg.a@mm.html**

"War of the Worms"

The authors of Beagle and Netsky have been sparring with each other, creating ever more powerful versions of their viruses and multiplying headaches for users. See **http://www.sophos.com/virusinfo/articles/wormwar.html** and **http://news.bbc.co.uk/2/hi/technology/3532009.stm** for details.

W32.Witty.Worm (affects ISS firewall products such as BlackICE)

This highly destructive worm, which was discovered on March 20, can corrupt hardware and damage files. For information about the worm, see **http://isc.sans.org/diary.html?date=2004-03-20** Information about the vulnerable products and patches is available at **http://xforce.iss.net/xforce/alerts/id/166** See also Symantec's report at **http://www.symantec.com/avcenter/venc/data/w32.witty.worm.html**

Virus Security Resource

To stay abreast of late-breaking viruses, see Symantec's comprehensive security site listing the latest virus threats at **http://securityresponse.symantec.com/avcenter/vinfodb.html**

— Other Threats —

Linux Servers Vulnerable

Three serious flaws have been discovered in Linux core software in the past six months. The flaws could enable an attacker to gain root privileges on a user's computer. For details, see **http://news.com.com/2100-1002_3-5162055.html?tag=nefd_top**

WinZip Hole Could Allow Attackers to Execute Malicious Code

Some versions of WinZip, a popular non-Microsoft utility for Windows that manages Zip files, have a serious security flaw that could allow attackers to execute malicious code. Users can protect themselves by turning off WinZip's automatic handling of Zip files in Windows Explorer and Windows XP. For details, see **http://www.eweek.com/article2/0,4149,1540280,00.asp**

DDoS Flaw Found in FreeBSD

All versions of the FreeBSD operating system are vulnerable to a denial-of-service attack unless they upgrade. For more information, including links to software updates, go to **http://www.internetnews.com/dev-news/article.php/3320751**

Social Engineering on the Internet: Protecting

What you don't know *can* hurt you! Learn how to steer clear of Internet tricksters

Jon Miyake
Acceptable Use Policy Officer
miyake@uoregon.edu

The purpose of this article is to help you understand what social engineering is and how it relates to the Internet—and to encourage you to think twice before opening that attachment, filling out that web form, or replying to that email.

1. "There's a sucker born every minute."

- David Hannum (often erroneously attributed to P. T. Barnum)

Social engineering is the creative mixing of truth, half-truths, or lies in order to extract information from you or encourage you to take a particular action. It happens every minute of every day in a variety of ways.

Social engineering skill is often colloquially referred to as good advertising, spin doctoring, or "hacking the wetware." Successful social engineering ploys do everything from luring you into divulging your credit card number over the phone, cajoling your boss into giving you a raise, or persuading you to buy a particular product or service. When social engineering is practiced with malicious intent, it's referred to as scamming or pulling a mark, and in the worst cases it is a federal offense.

Social engineering on the Internet. Malicious social engineering is false advertising. By combining false advertising with the selective use of known software flaws, it's easy to convince one person in fifty that something false is likely to be true—or is at least close enough to the truth to be worth the risk.

The Internet attracts many individuals to the dark side of spin doctoring because they can easily target a wider audience, get faster responses, and stay well out of reach of their irate victims. But even more alluring is the fact that the anonymity of the Internet allows an individual, no matter their creed, accent, hair color, or height, to become anyone they want to be. . .

2. "On the Internet, nobody knows you're a dog"

- Cartoon in the New Yorker

In cyberspace, nobody knows who you are or what you look like unless they've met you in person. You are represented only by your username and email address, and often your sole communication with a particular individual is via email.

Email is an increasingly important component in business and personal life. As a result, it's more common to think of a person by username rather than by first or last name. As your brain unconsciously creates these connections, the more likely it is that you're going to treat a message that purportedly comes from a person you know just as you would if it were handed to you in person. Unfortunately, the "From:" field in an email message is easily forged. This brings us to the third adage…

3. "Pay no attention to that man behind the curtain!"

- Wizard of Oz

Unless you're a sophisticated "uber user" (super user) or support professional, most underpinnings of your Internet service are invisible to you. Many network programs, email clients, and web browsers create beautiful façades that hide much of the data that can be used to determine their source and authenticity. In some cases, it's not so much the program's features that scammers and virus authors use to deceive you, but its flaws.

For example, suppose an uber user and an average user both receive an HTML (web-formatted) email message stating that their credit card company has had trouble sending paper billing. The email asks them to follow a link to an online form that will allow them to update their billing information. Each user reacts differently:

Average user's approach:

1. Reads the message
2. Looks at the sender's address
3. Clicks on the link provided and sees a professional website running a secure (SSL) web server that belongs to the user's well-known credit card company

Uber user's approach:

1. Reads the email carefully, looking for grammar and spelling errors
2. Looks at the message's full headers to determine its source
3. Copies the link into a web browser to view, and sees a professional website hosted in China that uses plain text as the SSL encryption method for an insecure webserver that definitely does not belong to the user's well known credit card company!

How do uber users see through the illusion?

- They use email and web browsing software that has a known track record.
- They don't click on links provided in an email message.
- If they're in doubt about the source of a message or attachment that purports to be from someone they know, they confirm its authenticity by phoning the sender.

For a real-life example of a recent spoofing incident of this sort, see "Bogus Banking Email Allows Trojan Infection for Outlook Users" at **http://www.auscert.org.au/3981**

4. "There ain't no such thing as a free lunch"

- Robert Heinlein

If it sounds too good to be true, it probably is! Think critically before acting.

Yourself from Con Games in Cyberspace

Viruses that Rely on Social Engineering

Many of the new viruses that are being seen both on campus and in the wild rely on social engineering to infect your computer. Although their viral payload can be assisted by features in such clients as Outlook or Internet Explorer, these viruses still rely on the user to help them propagate.

The W32.Beagle virus is a great example of a virus that depends on social engineering. The viral payload appears in the form of a file attached to an email message which purports to come from an administrative source. The message warns of a problem with your Internet or email service, and urges you to run the infected attachment in order to rectify the problem. Here are three sample Beagle virus messages with misspellings preserved:

— *"Our main mailing server will be temporary unavailable for next two days, To continue receiving mail in these days you have to configure our free auto-forwarding service."*

— *"Our antivirus software has detected a large ammount of viruses outgoing from your email account, you may use our free anti-virus tool to clean up your computer software."*

—*"We warn you about some attacks on your e-mail account. Your computer may contain viruses, in order to keep your computer and e-mail account safe, please, follow the instructions or your account will be disabled."*

Ironically, Beagle's diabolical virus-generated warning is actually prophetic. If you run the attachment, your email account or Internet connection *will* be disabled—not directly through the actions of the virus, but because your computer will begin spewing virus-laden email, prompting disconnection by the Computing Center's network security group!

To prevent viruses from propagating, UO network security staff routinely disable an infected machine's network access. During periods of high viral outbreak, restoring your network access may take the better part of a day.

Note that Computing Center support staff usually do not send attachments unless requested. Even then, the email message will most likely be cryptographically signed to bolster authenticity (for an introduction to PGP cryptography, see **http://www.pgpi.org/doc/pgpintro/**).

Hoaxes that Rely on Social Engineering

A common hoax that rotates in and out of circulation is the **jbdbgmgr.exe** or "teddybear" file hoax.

This hoax is propagated via email when one concerned colleague or friend forwards it another. The email explains that a trusted friend sent them a message warning them about an undetectable virus on their computer, an executable (**.exe**) file buried within their system files in the form of a teddybear icon. And indeed, when they checked their system folder, they found the infected file exactly as foretold.

In reality, the teddybear icon was the unfortunate choice of some developer. The file **jbalbalh.exe** is actually a java debugger that poses no real threat to your system, and deleting this file will not harm your computer.

Using Social Engineering to Go 'Phishing'

"Phishing" is the act of using Internet media, such as email and websites, to elicit sensitive information.

This is typically done by "spoofing" (emulating email or website formatting to masquerade as a well known entity, such as AOL, eBay, PayPal, Visa, and so on). In addition to their slick appearance, malicious websites or emails may take advantage of flaws in certain applications (e.g., Microsoft Outlook, Internet Explorer) to enhance their authenticity.

Nigerian 419 Scams: In some cases, such as the never-ending Nigerian 419 scams, greed is used as a motivator. As these scams have been circulating for the past 20 years, you are probably already familiar with emails that begin with entreaties such as, *"Dear honored sir, I am the son of the late dictator and I need someone to hold onto my money for me..."* The message goes on to request your personal banking information, promising a big reward in return.

Other common phishing ploys: Immediately become suspicious if you receive email messages such as:

-"Your account is about to expire please go to this website to re-enter your account and credit card information."

- We were informed that your card is used by another person or stolen. It could happen if you have been shopping on-line, and someone got your 'billing information' including your card number. To avoid and prevent any billing mistakes and to refund your credit card, it is strongly recommended to proceed filling in the secure form on our site and applying for our Zero Liability program. This program is free and it will help us to investigate this accident."

Conclusion

Don't trust a message or an attachment just because it appears to be from a familiar source. Don't be too quick to fill out a form on a website, especially if it asks for sensitive personal information that could be used in ID theft.

Forewarned is forearmed. Being aware of the ways in which social engineering is used to perpetrate Internet scams can help you avoid becoming a victim.

An Introduction to Appending Two or More SAS

If your study requires appending or merging datasets, you'll find SAS well suited to the task

Robin High
Statistical Programmer and Consultant
robinh@uoregon.edu

This article explains how to combine two datasets using SAS. We'll look at both appending datasets (resulting in an increase in the number of cases) and merging datasets (adding variables to existing cases). It is a condensed version of two much longer documents (**http://darkwing.uoregon.edu/~robinh/061appl_data.txt** and **http://darkwing.uoregon.edu/~robinh/062appl_merge.txt**).

Methods of Appending Datasets

To illustrate what we mean when we talk about appending two datasets, assume we have dataset alpha with variables *subject*, *age*, and *weight*, and dataset beta also with variables *subject*, *age*, and *weight*.

To use SAS to combine the data from those two datasets, one could simply enter:

```
DATA combo;
 SET alpha beta; RUN;
```

However, there are other more specialized SAS procedures which can also be used for this task, including:

- PROC APPEND
- PROC DATASETS (deprecated)

Choosing Between Using the SAS DATA Step Approach and PROC APPEND

Of the two approaches, the DATA step is the least efficient, although on today's fast systems, efficiency probably isn't a major concern for most reasonably sized datasets. The DATA step does have a distinct advantage in that it is the only method whereby SAS can compute new variables or enter conditional OUTPUT statements if there are any cases you want to delete. The DATA step also allows you to enter an option to keep track of which records came from specific datasets.

PROC APPEND. PROC APPEND also allows you to combine cases with the same variables, just as you can with a DATA step using a SET statement, but with more consistency checking.

By default, PROC APPEND takes special care to ensure that datasets to be combined are strictly congruent. It looks to see if all character variables are defined to be of the same length, and also checks both datasets to see if they have exactly the same set of variables.

You can override those PROC APPEND consistency checks if you want to (see the PROC APPEND FORCE option), but you should be careful when doing so. SAS is trying to help you avoid problems, so it's best not to ignore its efforts.

PROC APPEND comes in handy when you collect the same data over time or the same data from different sources and want to accumulate them into one file. PROC APPEND can also be used within a SAS macro where the same procedure is applied to many datasets and you need to place the results, such as regression coefficients or summary statistics, into one file. Other applications are found with simulations or bootstraps, where the output from many runs produce datasets with the same structure.

For examples and more detailed explanations of the various ways of appending SAS datasets, go to **http://darkwing.uoregon.edu/~robinh/061.appl_data.txt**

How to MERGE Two or More SAS Datasets

When you merge two datasets, your objective is to add new variables from matching observations.

For example, suppose you have a dataset called "states" that has information about each of the 50 states. That "states" dataset might have each state's name, its area in square miles, and its population. A new dataset, called "vehicles," has each state's name and the number of cars and the number of motorcycles registered in that state. You want to add the two variables from the "vehicles" dataset (the number of cars and the number of motorcycles) to the variables on the original dataset, "states."

In this case, each dataset has data for all fifty states. Both files should have one or more key variables with the same format. In our example, that would be the state's name. Other examples of common keys are Social Security numbers or subject names. The conservative way to do this is to create a new dataset (we'll call it "widedata") by entering:

```
PROC SORT DATA=states;
 BY state_name;
PROC SORT DATA=vehicles;
 BY state_name;
DATA widedata;
 MERGE states vehicles;
 BY state_name;
RUN;
```

Datasets or Merging Them Together

This example is comparatively simple, and does not fully reflect all the possible ways that the DATA step with a MERGE statement, or the even more powerful PROC SQL, can be applied.

Why Do You Need to Sort and Use a BY Statement?

If you merge two datasets without a BY statement, the process automatically matches data from row 1 of file1 with data from row 1 of file2, data from row 2 in file1 with the data from row 2 in file2, and so forth.

In some situations when SAS merges files without a BY statement, the process may work correctly. But what happens when you do not include a BY statement in the DATA step when it is really needed? SAS still processes the two files, but the resulting output dataset has incorrectly matched the records.

Because it is very easy to unintentionally merge variables from observations across two datasets that do not match, we recommend that you always first sort the two datasets by their unique identification variables with PROC SORT. You then enter the BY statement into the DATA step following the MERGE statement that lists the names of the two datasets.

If you're concerned that you might forget to include a BY statement when merging files, you can activate a System Option to report when a merge is missing a BY statement (this option will stop data processing):

```
OPTIONS MergeNoBy=error;
```

To summarize, you should always perform the following sequence of steps:

1. Sort the data first.
2. Use a BY statement following the MERGE.
3. Flag missing BY statements with a system option.

When merging files, many complications can arise. For example, you might encounter situations where you have multiple records in a file with the same value of the BY variable.

In such situations, the files can be combined, but only if you use very specific procedures. We strongly recommend that you print at least a sample of the resulting dataset to confirm that it merged the way it should. Details on some of the more complicated merge scenarios are available from **http://darkwing.uoregon.edu/~robinh/062appl_merge.txt**

Online References

1. "Everything you wanted to know about MERGE but were afraid to ask"
   http://support.sas.com/techsup/technote/ts644.html
2. "Reading, Combining, and Modifying SAS Data Sets"
   http://sas.uoregon.edu/sashtml/lrcon/z1125856.htm
3. "The SQL Procedure"
   http://sas.uoregon.edu/sashtml/proc/z0086336.htm
4. "How MERGE Really Works"
   http://www.pswcrl.ars.usda.gov/Popham%5Cmerge.pdf

Some Microsoft Products Conflict with ZoneAlarm

If you're using the network security software product ZoneAlarm to protect your computer from hackers, viruses, and the like, you may find yourself without Internet access after installing Microsoft Office updates.

According to Microsoft, installing a Microsoft Office Service Pack or upgrading to a newer version of Microsoft Office can disable some or all of a user's Internet connection if ZoneAlarm or ZoneAlarm Pro is running.

ZoneAlarm apparently recognizes the updated Office programs as new, unauthorized, programs and automatically prevents those applications from using an Internet connection.

How to fix the problem: To resolve this issue, configure ZoneAlarm to allow these programs access to the Internet. For assistance with this process, consult the ZoneAlarm help files or user manual (in particular, see the Programs FAQ at **http://www.zonelabs.com/store/content/support/zapProgramsFAQ.jsp#1program**).

If that fails, Microsoft recommends uninstalling ZoneAlarm and then reinstalling the product. Ideally, one would uninstall ZoneAlarm *before* applying the Microsoft Office updates, and then reinstall ZoneAlarm.

Visit Microsoft's Knowledgebase (accessible from **http://support.microsoft.com/**) and read article **315041** for more information. You'll also find a list of the Microsoft Office products and updates that are involved in this conflict.

Create Your Own Brand of Music with

Apple's new iLife tool eases you into the world of digital music

Patrick Chinn
Distributed Network Computing Consultant
pchinn@uoregon.edu

Apple brings the simplicity of cut, copy, and paste to music creation with GarageBand, a new component of iLife. GarageBand lets you assemble songs from supplied snippets of music, garnished with your own work.

Creating a song in GarageBand is simple: grab an audio loop from the loop browser and drag it to the track window. Each loop or instrument gets its own track (a track is a graphical representation of a timeline).

For instance, to create a drum line, pick a drum loop and drag it to the track window. Since the drum loop will need to play repeatedly, click and drag the end of the drum loop. GarageBand will automatically extend it, repeating the loop as many times as necessary to fill the time you indicate.

To augment the drums by adding, say, a cowbell, locate a cowbell loop in the loop browser. Drag the loop to the track window. GarageBand will place that loop in its own track. To play the cowbell loop at particular intervals, copy the loop and then paste it onto the timeline where you want the cowbell to play.

To hear the song, click the rewind button and then the play button.

Apple has taken steps to help prevent novices from creating a cacophony. GarageBand filters loops by tempo and key, reducing the chance that the selected snippet will clash with the composition. This feature is helpful for those of us short on music theory. Advanced users can disable the feature.

The inclusion of these musical snippets, called Apple Loops, is the fundamental difference between GarageBand and its more expensive competitors. Other programs rely on users to provide their own material. Apple's approach with GarageBand is similar to selling a word processor that includes pre-written paragraphs, leaving the "author" to assemble the paragraphs into a coherent document.

GarageBand supports recorded audio (samples) and MIDI (Musical Instrument Digital Interface). Apple refers to MIDI tracks as "software instruments," since the sounds produced by those tracks are software-generated rather than sampled. GarageBand also records live audio through the microphone or audio input. With the right cable or adapter, any instrument or sound source can be used to add audio to a song in real-time.

GarageBand also offers a collection of configurable effects like gate, compression, equalization, echo and reverb, which can be configured and applied to any track. For guitar players, Apple includes built-in guitar effects, including a variety of amplifier types (metal, scorching solo, seventies rhythm and ultra clean, for example). These amplifier settings effectively turn your Macintosh into a guitar amplifier.

The volume of each track can be adjusted over time. Each track has a volume line graph that can be manipulated to increase or decrease a loop's volume at various points as the song plays. Panning, on the other hand, has one setting per track and cannot be adjusted automatically.

To aid real-time recording, GarageBand has a metronome with count-in capability to keep you on the beat. The program also offers a rudimentary on-screen keyboard that can be played with the mouse cursor. This feature is of limited use; it's impossible to play fast passages of music and chords.

Apple also offers GarageBand Jam Pack. Jam Pack adds 2,000 loops, over 100 software instruments, over 100 effects presets and 15 guitar amplifier settings. These add-ons are integrated into Jam Pack during installation and are available through GarageBand's interface.

GarageBand is compatible with most any MIDI keyboard. To ease novices into digital music, Apple has been pushing an entry-level MIDI keyboard called the M-Audio Keystation 49e. The Keystation is a 49-key USB keyboard with full-size, velocity-sensitive keys (though 49 keys is far short of a full-length keyboard). The keyboard can be powered by USB, which allows you to conveniently leave the power adapter at home.

While GarageBand offers tools to edit MIDI data, these tools are rudimentary. The MIDI track editor allows a note to be moved left and right (through time) or up and down (in pitch). Pressing the command key turns the cursor into a pencil that lets you add notes by drawing them in the edit window. Strangely, there is no eraser to remove errant notes, and there is no convenient way to shorten or lengthen a note.

GarageBand's ability to edit sample loops is even more limited. You can split a loop into two pieces (set the cursor to the split point and from the Edit menu select Split). That's the extent of sample loop editing. If an imported sample needs more in-depth adjustments, you'll find it best to use another program like Audacity or SoundStudio (see sidebar).

GarageBand

Once you are finished with your song, GarageBand will export your creation to iTunes. (See "iTunes: Free Music Download Software is Much More than a Music Player." in the Winter 2004 *Computing News* at **http://cc.uoregon.edu/cnews/winter2004/itunes.html**) iTunes can be used to create a collection of your songs as an album and will burn that album to audio CD to share with friends and family.

To run GarageBand you need Mac OS X 10.2.8 or later and a DVD drive. Apple suggests a minimum of a 600MHz G3 processor, but to really use the software you will need a G4 processor. The more complex your composition, the faster your computer will need to be.

While GarageBand lacks some of the high-end features offered by its competitors, it is a great application to test the world of music—especially given its affordable price.

GarageBand is also a great solution for creating royalty-free music for class or iMovie projects. Overall, its an easy and fun program to use.

Audacity and Sound Studio: Two Editing Applications that Make a Good Companion to GarageBand

Editing recorded audio is a critical part of many media projects. Macintosh users on campus have two options for audio-editing applications: Audacity (freeware) and Felt Tip Software's Sound Studio (shareware; UO site-license).

These programs both record and edit audio. For instance, let's say we have recorded a wonderful bit of audio but need to remove extra audio from the beginning and end of the clip. Both programs make this kind of edit as simple as click, drag, and delete. Need to adjust a clip's volume? Use the "normalize" or "compress" filter on some or all of the sound clip.

Both applications make a good companion to Apple's GarageBand. While GarageBand can also record and edit audio, its editing features fall far short of those offered by Audacity and Sound Studio.

In addition to editing clips, Audacity and Sound Studio also offer various effects like chorus, flanger, delay, echo and reverb. (Other effects are available, but they are too numerous to list here.)

Audacity also supports VST audio plug-ins, while Sound Studio does not. VST plug-ins extend the product's abilities without increasing the price by adding additional effects or processing options. Audacity also supports multiple tracks, while Sound Studio assumes you need either mono or stereo (one or two) tracks.

Sound Studio lacks the ability to save files directly to MP3 format (one common computer music file format). Felt Tip Software has avoided licensing MP3 technology and recommends using iTunes to convert AIFF audio to MP3. Sound Studio will import MP3 files by using the "Import with QuickTime" command on the File menu. Audacity, on the other hand, will open and save MP3 files without any extra steps.

Sound Studio may lack some of Audacity's features but Sound Studio's interface is better designed, making it a better match for audio beginners. Knowledgeable users will find Audacity's powerful features more to their liking.

Download Audacity (Mac OS X, Windows and Linux) at **http://audacity.sourceforge.net/** This page also has a link to the VST-compatible plug-ins.

Sound Studio is available (for Mac OS 9 and Mac OS X) at **http://www.felttip.com/products/soundstudio/** , but note that this software requires a license. The Yamada Language Center has purchased a site license for the UO. For licensing information, please contact Jeff Magoto at *jmagoto@uoregon.edu*.

More Selected Elements of the University 2003 Home Page Study

The last in a three-part series on the evolution of university websites

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

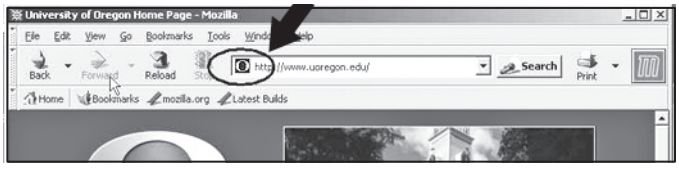
At the request of the UO administration, we conducted a comparative study of 172 university websites in the summer of 2003. (For a complete list of the universities studied, see **http://darkwing.uoregon.edu/~joe/2003-web-study/sites.txt**)

In the Fall 2003 *Computing News* (**http://cc.uoregon.edu/cnews/fall2003/webstudy.html**) we discussed some of the mechanical issues associated with university web page delivery, including "natural minimum web page sizes" and the web servers and Apache modules universities chose to use. In part two (**http://cc.uoregon.edu/cnews/winter2004/webstudy2.html**), we looked at some design trends in higher education home pages. In this final segment, we'll examine the use of specific technologies such as favicon.ico, Platform for Privacy Preferences files, and robots.txt files.

Some Specific Features of Web Design

I. favicon.ico use

A number of web browsers enable a website (or an individual web page) to specify a small 16x16 "favicon.ico" graphic which should be associated with a website that's selected as a "favorite" or "bookmarked" website. When this feature is used, the presence of a graphic logo can make it easy to pick a favorite site out from a long list of web pages, and it is an easy-to-add enhancement for most websites. Here's an example of what a favicon.ico looks like (in the address field of the UO home page):



To assess the extent to which favicon.ico had attained critical mass, we checked each of our study sites to see if they had a favicon.ico file in the default location. We found that 48 sites (28%) did, and 124 sites (72%) did not, have a favicon.ico file.

We're somewhat surprised to see so many sites miss such an easy and obvious "branding" opportunity. (For more information on the favicon.ico feature, see **http://msdn.microsoft.com/workshop/Author/dhtml/howto/ShortcutIcon.asp**)

II. Platform for Privacy Preferences

The Platform for Privacy Preferences Project, a project of the World Wide Web Consortium (**http://www.w3.org/P3P/**), has endeavored to make it easy for a site to succinctly express its privacy policy via a standardized file.

We tested each of our study sites to see if they had created a non-zero length file at **http://www.<domain>.edu/w3c/p3p.xml** by trying to retrieve that file.

Two sites had a suitable file: SUNY Stony Brook and Virginia. In other cases, a custom error page was returned when the special **p3p.xml** page wasn't found. This occurred in the case of Cal Tech, Clark, Clemson, Catholic, Dayton, Fordham, Marquette, Miami (Ohio), Missouri (Kansas City), Nebraska (Lincoln), Nevada (Reno), New Jersey Institute of Technology, Southern Methodist, SUNY ESF, UCLA, and Wyoming. The other study sites did not have a P3P file.

III. robots.txt file

Yet another bit of standardized meta data is the **robots.txt** file, designed to control what does, and does not, get indexed by search engines such as Google and Altavista, (see **http://www.robotstxt.org/wc/robots.html**).

101 of our 172 study sites had a "real" robots.txt file. In seven cases, similar to the situation for the **p3p.xml** file at a number of study sites, requesting the robots.txt file returned a custom 404 ("page not found") error page instead of a "real" robots.txt file. The seven misbehaving sites were Clemson, Dayton, Nevada (Reno), Southern Methodist, SUNY ESF, UCLA, and Wyoming.

When robots.txt files *were* present, they were generally configured to do one or more of the following:

- to keep robots and spiders out of cgi-bin directories, log/stat directories, test/trial/development/temporary subdirectories, old/out-of-date data directories (such as old copies of a university's catalog) or other content that might index badly, be misleading or confusing, or have low information value
- to keep robots out of phone book, financial aid, budget, personnel, and medical data, or other "confidential" stuff (although robots.txt offers pretty poor protection when it comes to sensitive information!)
- to deter spammers from harvesting addresses by listing selected User-agents by name (although there's some question as to the extent that email address harvesting bots respect robots.txt files!)
- at some sites, to prevent indexing of class web pages (possibly because the pages which would otherwise be indexed are mock-ups of fictitious commercial websites)
- in some cases, to inhibit "indexing" of gifs, jpegs, and other images
- in another case, to prevent indexing of any personal web pages hosted at that university

In general, even if you're not a robot, **robots.txt** files can be fascinating to review!

OpenVMS Licenses Available Free for Educational and Hobbyist Use

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

Most of our readers are aware that Linux and various BSD operating systems (FreeBSD, NetBSD, etc.) are freely available. But what you may not know is that free OpenVMS licenses are also available for hobbyist and educational uses.

For details about the OpenVMS free licensing program, please see:

http://www.openvmshobbyist.org/

and/or

http://h71000.www7.hp.com/openvmsedu/index.html

Note that there are some requirements that must be met:

- modest media charges may apply
- OpenVMS will only run on specific VAX/Alpha/Itanium hardware
- the license program grants only year-long (renewable) licenses

Despite such requirements, this is still a fantastic opportunity for those of you who may be interested in trying OpenVMS.

« sites worth seeing »

1. **TopoZone Pro…** A site of interest to professional and recreational map users. Provides shaded relief maps, high resolution aerial photography, and street maps, among other features. TopoZone is also a source for custom digital topographic data for web, GIS, and CAD applications.
   http://www.topozone.com/
2. **GPL Code Center…** Download site for Lynksys wireless access point source code.
   http://www.linksys.com/support/gpl.asp
3. **iBook Logic Board Repair Extension Program…** Apple's resource for covering repair or replacement of the logic board in specific iBook models manufactured between May 2002 and April 2003.
   http://www.apple.com/support/ibook/faq/
4. **"Using Blosxom to Create a Weblog on Darkwing"…** Mary Harrsch, network and information systems manager for the UO College of Education, shares her insights, including links to templates for setting up a basic blog.
   http://interact.uoregon.edu/techweb/Blosxomcreation.html
5. **"Can you trust 'trusted computing' ?"…** One writer's critique of Microsoft's Trusted Computing project.
   http://techrepublic.com.com/5100-6313-5081241.html
6. **"Virginia Tech's Power Mac G5-based 'X' Supercomputer is officially number 3 in the world"…** A review of Virginia Tech's top-rated supercomputer project with Apple, Mellanox Technologies, Liebert, and Cisco. Its supercomputer, 'X,' is the fastest university supercomputer in the world.
   http://www.spaceref.com/news/viewpr.html?pid=13072
7. **"Is Your E-mail Campaign Being Blocked or Filtered by ISPs?"…** Brackin's Message Checker service and related products can monitor whether or not legitimate messages are getting through.
   http://www.brackinsystems.com/hm/index
8. **"I fought the scammer… and I won"…** John Allman's account of his successful sleuthing at a Dublin Internet cafe.
   http://www.linux.ie/pipermail/ilug/2004-April/013049.html
9. **Special Report on "Phishing"…** A comprehensive report prepared by the Criminal Division of the U.S. Department of Justice about the risks of responding to "phishing" emails and websites. Also lists steps users should take when they see suspected phishing emails and websites.
   http://www.antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.pdf
10. **Special FDIC consumer fraud alert…**Beware of spurious email that appears to be sent by the FDIC claiming that Homeland Security Director Tom Ridge has advised suspension of all deposit insurance on your bank account due to suspected violations of the PATRIOT Act. Such email is part of a "phishing" scheme to obtain sensitive personal information and should be ignored.
    http://www.fdic.gov/news/news/press/2004/pr0604.html
11. **"Paid to Spam"…** A discussion of Virtual MDA's offer to pay people to run their spam relay program. (Participation in any scheme of this sort is of course strictly forbidden by the UO's Acceptable Use Policy, and will result in sanctions if detected.)
    http://yro.slashdot.org/yro/04/04/14/1415217.shtml

COMPUTING CENTER GUIDE

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

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

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

(151 McKenzie Hall)

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

346-4412
microhelp@lists.uoregon.edu

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

(175 McKenzie Hall)
346-4406

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

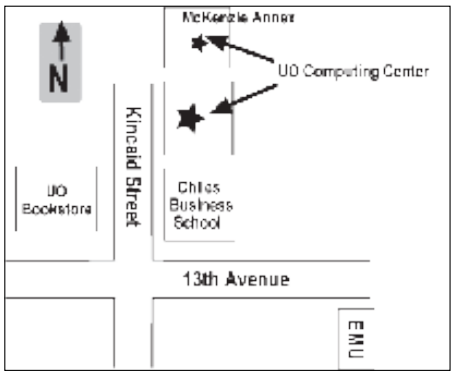
Large Systems Consulting
http://cc.uoregon.edu/unixvmsconsulting.html

(225-239 Computing Center)

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

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

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



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

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

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

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

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

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

Computing Center Hours

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

McKenzie Building Hours

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

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

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