

# The South Bay Mug

# MAGINTOSH

A Monthly Cupful For South Bay Apple Mac User Group Members, Nov 2007

## MACHinations

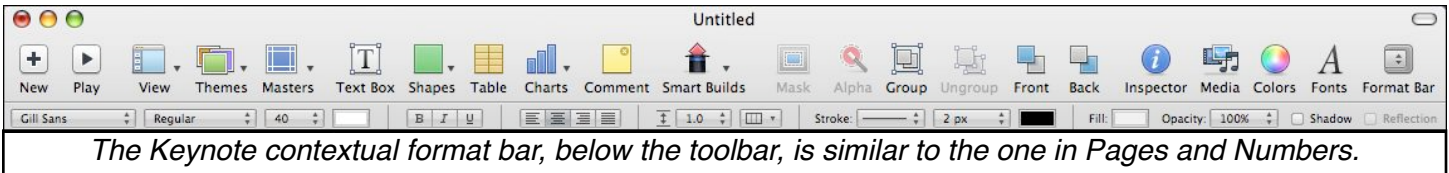
A personal view from Bob

### iWork '08

**I**Work '08 now comprises three programs, Keynote, Pages and a new entry, Numbers, and sells for \$79. I've been using iWork since Keynote was introduced four years ago, but have only used iWork '08 for a few weeks. It's definitely the best yet. Although very similar to earlier versions, it sports many new features, making it a worthwhile upgrade. All three programs are very easy to use and include a large number of templates or themes and share a similar interface. Operations are invoked using the Inspector, Text and

podcast. Presentations export as QuickTime, Powerpoint, PDF, a set images, a Flash movie with sound, HTML or to your iPod. Files created by the new version can't be read with earlier versions, but you can save a presentation as a Keynote '05 or '06 file.

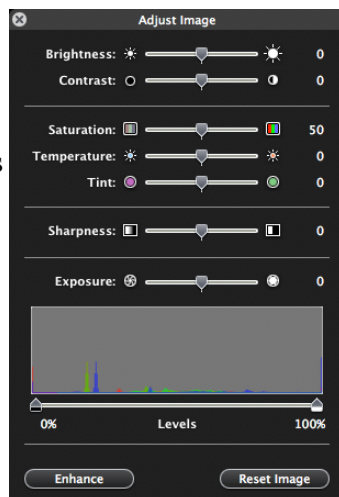
**Pages** is a word processing program that I use for my newsletter articles. When opening a new document choose between word processing and page layout. The latter is like the draw module in AppleWorks with linked text boxes and graphics. Control-click any word to correct spelling or look it up in the Dictionary, Thesaurus, Spotlight, Google or Wikipedia. Export as a PDF file, Word document, or text. It opens, but doesn't save AppleWorks 6 files. You can send it to iWeb but I didn't see any way to create an HTML page.



The Keynote contextual format bar, below the toolbar, is similar to the one in Pages and Numbers.

Color palettes. New in iWork '08 is a contextual format bar (see above), saving a trip to the Inspector. There's now an image adjustment palette for graphics (see below and think iPhoto).

**Keynote** is what I use for my presentations. I prefer it to Powerpoint because of its powerful graphics capability. It's easy to mask an image, add a picture frame, make a background transparent and add text shadows and reflections. Create charts from a table of numbers. I even use it as a drawing program. Making slide transitions, text and object animations, and object builds has been simplified. Add audio narration and make a self-running slideshow or video



**Numbers** (spreadsheet) is the new kid on the block, rounding out the iWork suite. Most spreadsheets are boring pages of rows and columns. Numbers is a free-form page-layout program that includes resizable spreadsheets along with photos, text, charts and drawing elements to make a gorgeous presentation. Numbers is not for accountants or spreadsheet jockeys, but rather for the home or small business user. Numbers has 168 useful mathematical functions (100 less than Excel), fewer graph types and no macros, but is very easy to use. It opens and saves in the Excel format, including the new file format in Office 2008. I opened a couple of large, uncomplicated, Excel documents and they converted flawlessly.



**Bob Brooks**  
Helping Beginners  
310-545-8060  
SBAMUG@gmail.com



# Welcome to South Bay Apple Mac User Group

You and your friends are invited to attend our next meeting. Our membership dues are only \$35 per year, entitling you to this newsletter each month and many more benefits. If you would like to become a member or get more info on SBAMUG, feel free to check out our web site at:  
[www.sbamug.com](http://www.sbamug.com)

P. O. Box 432  
Redondo Beach, CA  
90277-0432

310-644-3315  
Email: [info@sbamug.com](mailto:info@sbamug.com)

## Meetings are held at the

Redondo Beach Community Center  
320 Knob Hill, Redondo Beach  
(see map & directions on page 11)

---

### Officers & Volunteers:

President:.....LJ Palmer  
Vice President:.....Jim Pernal  
Secretary:.....Wayne Inman  
Treasurer:.....CW Mitchell  
Directors at Large:.....Dave Nathanson,  
George Kiefer, Dorothy Weeks, Louise Polsky,  
Chuck Mulvey, Jayne Palmer  
Membership Director:.....CW Mitchell  
WebMaster & User Group Ambassador:  
.....Bob Brooks  
Server Director:.....Dave Nathanson  
USPS Liaison:.....Don Myers  
PD Disk Editor:.....Jim Pernal  
Program Director:.....George Kiefer  
Newsletter Editor:.....Dorothy Weeks  
Raffle Chairman:.....George Griffiths  
Raffle Director:.....Chuck Mulvey  
RefreshmentCoordinator:..Louise Polsky, Taffy Rath

### Membership Report:

(You may notice your name is in larger letters  
on your card. That is so it can be used as a  
name tag at the meetings.

Your Membership Cards are in the mail!)

**Current Membership - 165**

### Thank You Member Renewals -

Amy Wasserzieher, C. M. Stubben, Karin  
Petersen, David Nathanson, George Kawahara,  
John Fahey, Benjamin Bundoc, Al Tucker,  
Alverda Ferguson, Gene Knell.

Remember, if your name is not spelled right or  
your expiration date is wrong, contact  
[cwmitchell@sbamug.com](mailto:cwmitchell@sbamug.com) for correction.

---

### MONTHLY CALENDAR

**1st Sat - SBAMUG Core Group Mtg @ announced locations, 10 am**

**1st Thur - LB Mug @ Emerson School, Palo Verde & Willow, Long Beach, 7 pm**

**1st Sat - Orange Apple UG, Orange Coast College, Chem Bldg, Costa Mesa, 8am-1pm**

**3rd Sat - Adobe Tech Exchange Toyota Bldg on Grammercy near 190th, 9 am; \$10**

**Last Wed - SBAMUG Monthly Meeting**

**Last Tues - WOCMUG @ Emerson School, Palo Verde & Willow, Long Beach, 7 pm**

**Last Sat - TRW / Northrop Ham Radio & Computer Swap Meet, 7 am - 11:30 am**

---

The SOUTH BAY MUG (ISSN 1058-7810) is published monthly for \$35.00 per year by South Bay Apple Mac User Group, 2550 Via Tejon, Suite 3J, Palos Verdes Estates, CA 90274. Periodicals Postage Paid at Palos Verdes Peninsula, CA and at additional mailing offices. POSTMASTER: Send address changes to THE SOUTH BAY MUG, P.O. Box 432, Redondo Beach, CA 90277-0432.

The South Bay MUG is published by the South Bay Apple Mac User Group (non-profit). Excerpts may be reprinted by user groups and other non-profit media. Credit must be given to SBAMUG and the author. In addition, a copy of all reprinted materials must be sent to us at the address listed above. The South Bay MUG is an independent publication not affiliated or otherwise associated with or sponsored or sanctioned by Apple® Computer, Inc. The opinions, statements, positions and views stated herein are those of the author(s) or publisher and are not intended to be the opinions, statements, positions or views of Apple® Computer, Inc.

**Members are invited and encouraged to submit articles and original artwork for publication. Newsletter deadline is the last Wednesday of the month. Articles may be edited to fit in available space.**

Please send to: [dhweeks@sbamug.com](mailto:dhweeks@sbamug.com)

## SBAMUG November 2007 PD CD

Eight programs this month. Some are updates of older programs that are done for compatibility with the new Leopard OSX 10.5 operating system.

**iGTD.dmg** "I get things done," an organizer. Lets you set start and due dates, priorities, name, project, etc. Add a list of task notes. You can either have this program sync with iCal or not. Calendar in the lower right. Requires OSX 10.4 PPC/Intel.

**Mactracker.dmg** Latest version 4.3.1. Released in August, it has the Summer 2007 new Macintoshes. This great database has all the info on Apple computers, keyboards, monitors, printers, scanners etc. OSX 10.3.9 or better. Freeware

**Boinx\_Mousepose\_2.5.2.zip** This utility will place a bright spotlight around your mouse pointer and dim the rest of your screen. You can adjust the dimming, spotlight size, and edge blur. Updated to run on 10.5 or you can run it on 10.4 Shareware

**Pacifist\_2.5.1.dmg** Extract items from installer packages. An example is if Preview is either thrown out or is damaged. You can then go and just extract the Preview application, rather than going through a complete re-install of the operating system. OSX 10.3.9 -to the new 10.5. Just updated for 10.5

**1Password-2.5.2.dmg** Keep track of all of your passwords in one location. Shareware, OSX 10.4 10.5 on PPC and Intel based Macintoshes.

**pipette-universal.zip** One trick pony, as they say, to get color pixel information in the hex RGB format. Drag the eyedropper off the application window to any area of your desktop to select a color. Click and the value shows up. You then copy and paste. Good for web developers, or in programs like Photoshop Elements.

**SimpleComic\_1.6\_147.zip** Image viewer aimed at viewing comics. You can change order (left to right, right to left), rotation, scale, and or zoom in on details. Handles a variety of graphic formats. Freeware. OSX 10.4 to 10.5. PPC/Intel

**SlideshowMovie\_1.0.3v14.dmg** Shareware program lets you build up slideshow movies from a group of images. Lots of transition effects. Movie is self-contained. You can add watermarks to the images/photos. Requires OS X 10.4

The CD for this month will be at the December meeting as the November-December 2007 CD.

Catch you at the November meeting.  
*Jim Pernal* PD Editor

\*\*\*\*\*

## Searching Just Your Bookmarks

If you're trying to search for a particular bookmark, you'll want to know this trick: First, click on the Show All Bookmarks icon in the top-left corner of the Bookmarks Bar. Doing this makes the Collections column visible on the left side of Safari, but more importantly, it adds a Search field at the bottom center of the Safari window. When you type search terms in this field, it searches just within your bookmarks, so you get super-fast results.

*Courtesy of apple.com*

\*\*\*\*\*

## Hope You Noticed...

Did you take a look at the new list of officers and board members of the Core Group listed on p. 2, opposite this page? These folks keep the SBAMUG running, along with the help of many of the rest of us. If you can offer some help, please let us know. We always need help with refreshments, set up, clean up, topic ideas, hosting the Core Group, and lots more.

## The Best (and Worst) of Leopard

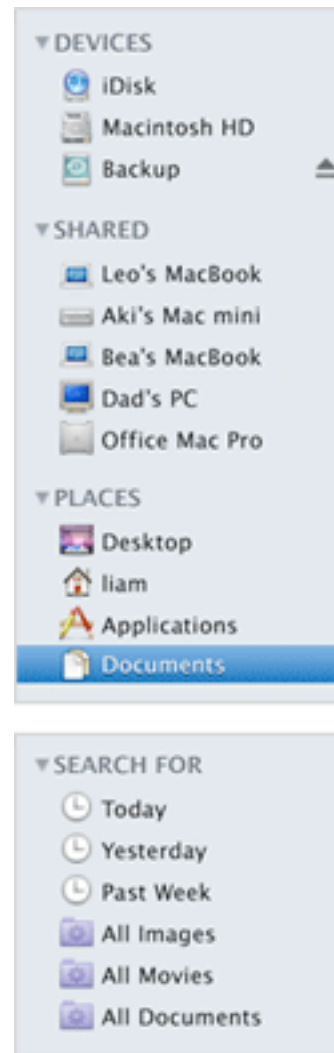
by *Matt Neuburg*, courtesy of *TidBits.com*

Before we go any further, may I say that I've been giving the Big Cat nomenclature problem some serious thought - Jaguar, Tiger, Leopard, how long can this go on? Well, I've discovered that there are a whole bunch of African feline species I'd never even heard of, such as the [Caracal](#) and the [Serval](#). So at the current rate of development, this should carry Apple forward for at least another decade - by which time, if present trends are any indication, further species will have been discovered (or they'll all be extinct, one or the other).

Okay, to business. Apple has finally locked down the ship date for Leopard (just as Adam predicted in "[It's Official: Leopard Ships on October 26th, 2007](#)," 2007-10-16), and posted its [list of over 300 new features](#). Now, I'm still under a non-disclosure agreement that says I can't talk about anything Apple hasn't told you. But since Apple *has* told you about the 300 features, I can talk about them. I can't add any new information, of course; but I can tell you how I feel about them (Apple doesn't own my feelings, as far as I can tell). Here, then, are my favorite (and least favorite) new Leopard features.

Let me start with the bad news - what I don't like. There is just one thing, really, but it's quite a big thing, namely: the Desktop's new look.

It's like the emperor's new clothes. A menu bar that's hard to read because what's behind it shows through? Why is that a good idea? And stacks in the Dock are a solution in search of a non-existent problem; the way folders behave in the Dock now (just click and the folder opens, click and hold to see a hierarchical menu of the folder's contents) is great and doesn't deserve to change. Not to mention the whole distracting silly way the Dock is now being drawn. I already dislike the Dock and do all I can to keep it hidden all the time; in Leopard, I'll have twice as much reason to do so. The new Finder window sidebar is awful too; you can see in [Apple's own screen shot](#) that the icons and text are tiny and all the colors are converging on basic gray.



- Now that I've got that off my chest, here are the new features I like the most. I'm not saying there aren't other cool new features, especially within individual Apple applications; but these are the features to which I truly look forward, the ones that actually make me eager to start using Leopard:
- Spaces. It's fun. It's easy. It works. I'm going to use it! Spaces will genuinely help me handle the clutter when I'm working in multiple applications with lots of windows open. Unfortunately, [Apple's Web page](#) on the topic doesn't do it justice - and I can't describe it for you, because I can't say anything they don't say.
- Time Machine. Okay, maybe it's not as

powerful as whatever super-snazzy network-based case-hardened backup system you're using at the office. But Time Machine is a great idea: simple, automatic backup that takes away all excuse for not being able to find some file you threw away two hours ago, or for not having an extra copy when something goes wrong. Even more important, if I screw things up really badly, I can restore the *whole computer* to a previously saved state. It really *is* a time machine! I can already feel my hair returning.

- The Path Bar. It shows you where you are in the Finder, at any given moment. Simple, elegant, obvious, and we should have had this years ago. Yes, I know you can Command-click the title bar to get the same information; but my mom, and a lot of other users, do *not* know this.
- Quick Look and Cover Flow. Together, these offer file previews on steroids. They're utterly silly ("waste cycles drawing trendy animated junk" was my first thought) until you need them, and then they are just terrific. Being able to flip through a bunch of music or photo files looking for the right one, right in the Finder without starting up any other application, is really great.
- Spotlight, Spotlight everywhere. Unfortunately, Apple doesn't mention what I think is the most important change to Spotlight, so I'm not allowed to tell you what it is. Suffice it to say that previously I didn't like Spotlight very much, and now I do, so obviously they must have changed the thing about it that I didn't like, right? Plus, I will now be able to search the past! With Safari, I can search for Web pages I've viewed, using whatever text within those pages I happen to remember. With Time Machine, I can search for files that no longer exist. Now if I can just find that \$20 bill I had a week ago.
- Share and share alike. The new easy built-in screen sharing, and the new easy way of sharing specific folders, are going to be a

boon for me in my ordinary home-networked, multi-computer environment. I also look forward to being able to view someone's desktop through iChat. Plus there's now a built-in Guest account that's automatically purged when the user logs out, making it safe and easy for me to share my computer as well.

- Mail turns into a powerhouse. RSS, to-do items, and miscellaneous notes are now incorporated right into Mail. No need to switch to iPhoto to find a picture and add it to a message. Easy mailbox archiving. I've switched mail clients several times in the past, and these improvements might be enough to get me to switch once again - to Apple's own Mail application.
- Improvements to AppleScript, Automator, and Xcode. Okay, these are totally nerdy, and they won't matter one whit to you if you're not a programmer at some level. But as you probably know, I wrote a [book about AppleScript](#), with some mention of Automator and Xcode; and I've done some work with Xcode and Objective-C, such as my popular free utilities [NotLight](#) and [MemoryStick](#). So, Nerds 'R Us! A truly Unicode-savvy AppleScript will end a text-handling nightmare that's been with us since the dawn of Mac OS X. Automator's new "Watch Me Do" feature is like making your mouse-clicks recordable. And there are lots of other toys, such as improved design, editing, debugging, and analysis tools, that will make any Xcode developer drool.

In just a few days all these improvements will be *mine*. (Rubs hands with evident glee.) Oh, and did I mention that instructions on using some of these features (and more) will be in my forthcoming "[Take Control of Customizing Leopard](#)" ebook? You can't have a copy yet, since Apple would have my head for revealing cool stuff ahead of time, but you can pre-order it now (and then download the full version as soon as Leopard becomes available).

## What'd I Say

by Chico

Hey Now! I bought a 50 foot audio cable from Monoprice (monoprice.com) to connect my stereo receiver to my Mac for a vinyl to CD project. It cost \$10, including shipping. The equivalent cable at Radio Shack (actually three 16 footers) was \$51. Thank you LJ.

*The Visual Display of Quantitative Information* is a classic book by Edward Tufte (The Da Vinci of data, the Galileo of graphics). If you find this topic interesting, check out the amazing maps recommended by one of our members at strangemaps.wordpress.com. Incidentally, for reasons I have yet to research, Tufte is highly critical of Powerpoint.

The Renaissance Person of the Month is Gregg Easterbrook, an author and contributing editor of *The Atlantic Monthly* and a visiting fellow in economics at the Brookings Institution. His best known book is *The Progress Paradox*, in which he explores how our lives have vastly improved in the last century, yet we tend to be pessimistic about the present and future. It's okay, but where Gregg shines is as the Tuesday Morning Quarterback, every Tuesday during the football season, at [espn.go.com](http://espn.go.com). He rehashes all the Sunday NFL games with emphasis on the brilliant strategy moves of the good coaches (Bill Belichick) and the moronic decisions of the bad coaches (all of them not named Belichick). He also features some of the more photogenic cheerleaders (nothing salacious). Interspersed in all this are fascinating detours into astronomy and archaeology. His interests are myriad.

What do you say? If you have a favorite website, podcast, Youtube clip or other tidbit or a nominee for Renaissance Person of the Month, please contact [chico@sbamug.com](mailto:chico@sbamug.com).

## Combine PDFs

Courtesy of NCMUG, April 07

It's extremely easy to make PDFs, as I explained in *How to make PDFs in OS X* (FBAMac Tip #97/16-April-2003). Recently though, I made a PDF from one Microsoft Word document that was divided into several sections, each with separate page numbering. I was rather surprised to find that instead of a single PDF, there were four. Obviously this was related to the use of sections in the source file.

After some Googling around how to combine the PDFs into a single file. I turned up the free Combine PDFs, which worked well. I opened Combine PDFs. It displayed a window. I dragged each PDF onto the window in turn, making sure to drop each below the previous, so as to keep the pages in order. The software displayed each page from each PDF, providing the opportunity to remove pages or change the sequence.

When done, I edited the Title, and Author information and pressed the Merge PDFs button. Moments later I had a single PDF of some 340 pages. Brilliant!

When I posted about this on my blog one reader, Derek Miller, kindly pointed me to another, similar piece of software called PDFLab, also free. I downloaded it and tried it out. It worked in the same way and I was very satisfied. If you need to combine PDFs, then try out either or both of these two fine pieces of freeware.

From: <http://mactips.info/tips/> 4 April 2007  
'Courtesy of NCMUG, April 07

Editor's note: Combine PDFs is invaluable in putting together this newsletter you're reading!  
DW

\*\*\*\*\*

**HAPPY THANKSGIVING  
TO YOU ALL!**

## Installing a New Operating System

*Bob Brooks, from the Beginners Group*

When you install a new OS, e.g. Leopard, you have choices:

Update just replaces the old files in the OS with new ones. This works OK unless you have some corrupt System files that get carried over to the new OS.

Archive and Install replaces the System folder with a brand new one but retains everything else. The old System folder is renamed "Previous System" in case there are some user installed files that you need, e.g. special fonts.

Erase and Install wipes out everything and installs the new OS.

I hope I've got this right. In any case make sure you have a complete backup first. If you clone your computer to an external, bootable Firewire drive you can restore your computer if things go haywire or you find you don't like Leopard.

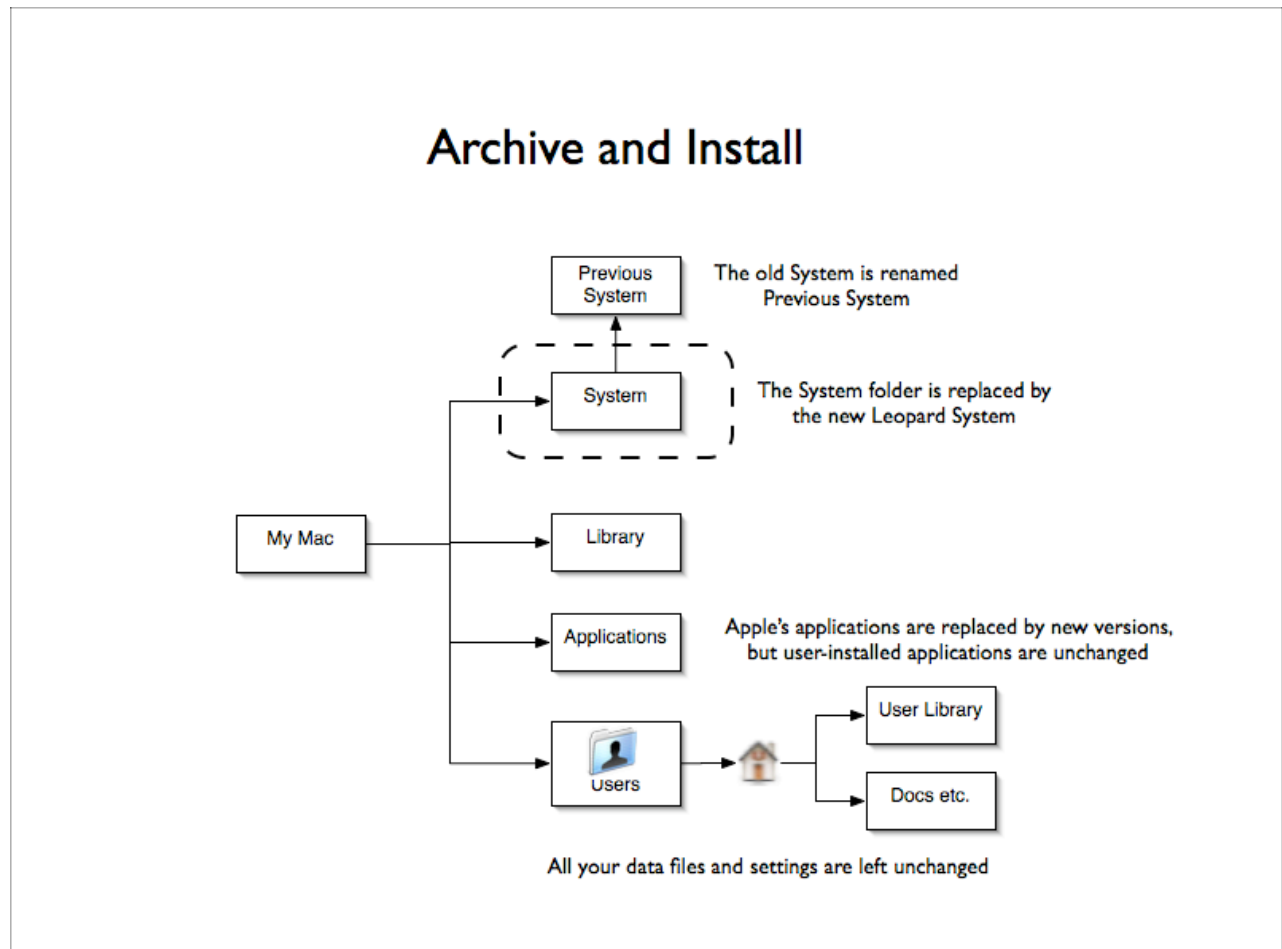
## Mac Treat # 26: How To Use Text Clipping

*By Ed@Smalldog.com*

Here's an old "trick" that many new Mac users are unaware of. This is an extremely fast and easy way to "grab" a chunk of text from almost any application (Safari, Firefox, Word, Mail, etc) and drop it onto your desktop as a "clipping." The text clipping can later be opened and read, or pasted into any word processor. This is handy for grabbing a quote off the internet, for example.

To do this, all you have to do is highlight the text you wish to "clip" by dragging your mouse over it, then click on this highlighted text and (without letting go), drag it to the desktop. Now, on the desktop, you'll have a new file containing the text clipping. You can use this text as you'd use any other text file. Note that you can also drag this text directly into the word processor of your choice, or even into Mail.

Once Mac users start using Text Clippings, it's a shortcut that people use on a daily basis. Give it a try!



## How Leopard Will Improve Your Security

By *Rich Mogull*. Courtesy of *TidBits.com*

With the release last week of [the feature list for Mac OS X 10.5 Leopard](#), the security world is buzzing about some extremely important updates that should, if they work as expected, significantly improve Mac security and will make me less nervous about connecting to wireless networks in Internet cafes.

**Time Machine** -- Before we dig into Leopard's advanced anti-exploitation technologies, we need to start with the biggest security feature that's not listed with the rest: Time Machine. Information security is based on the principles of CIA. No, not the Central Intelligence Agency or the Culinary Institute of America. In the security world, CIA stands for Confidentiality, Integrity, and Availability. While we tend to focus on keeping people from seeing things we don't want them to see (confidentiality) and changing things we don't want changed (integrity), having our data and systems available to us is just as important.

With Time Machine making it easier to back up for all users, especially individuals not already protected by some corporate backup system, Apple is doing more to improve security than any upgrades to firewalls or Safari ever could. If you want to improve your security, I highly recommend you get an external hard drive with your copy of Leopard (Adam tells me that "[Take Control of Customizing Leopard](#)" will offer basic help for Time Machine, and a future edition of "[Take Control of Mac OS X Backups](#)" will provide even more detail). My backups have saved me three times already this year, and I'm excited that I can finally make backups more accessible to my mother and sister.

**Stopping Buffer Overflows** -- The most significant security update in Leopard is one that you'll never notice, but that will cause the bad guys no end of frustration. It's an anti-exploitation technology Apple calls Library Randomization (also known generically as Memory Randomization and as Address Space Layout

Randomization in Windows Vista). To understand Library Randomization we need to take talk about vulnerabilities, exploits, and buffer overflows.

Buffer overflows are the class of vulnerability that are responsible for most of the successful attacks on computers today. Most malicious programs (worms and viruses) rely on buffer overflows to take control of your system. In security, we define a vulnerability as a flaw or defect that could allow someone to violate confidentiality, integrity, or availability. Think of it as a weak lock or a broken window the bad guy can use to get in. Buffer overflows are a vulnerability where an attack enters more data into an input than expected; if the programmer who wrote the software forgot to limit that input field, the data can flow past the expected limit and overwrite other parts of memory. Since memory on most of our computers is just a big stack of commands mixed with data, if you know exactly how much extra data to put in, you can trick the computer into running an arbitrary command by overwriting a spot where it expects a legitimate instruction with your new instruction.

You might be asking yourself why programmers don't just cap any program input to prevent buffer overflows. Why not just limit all those fields so this can't happen? I often ask myself the same question, but modern computing systems are so complex, with so much reused code, that it isn't that simple. For example, [the iPhone 1.1.1 software was cracked](#) because it used some common code (the libtiff library) for reading TIFF image files. That code had a buffer overflow vulnerability in it, allowing hackers to create special TIFF files that let them take over the iPhone. This is what we call an exploit - when you can take advantage of a vulnerability and actually do something with it.

As an aside, buffer overflows first appeared around 1988 and were used in the very first Internet worm - [the Morris worm](#). In 1996 [an exceptional paper was published](#) detailing how to exploit buffer overflows.

This is where Library Randomization comes in. Pushing those bad commands onto the stack is



more complex than saying, "Open sesame!". The attacker is attempting to subvert the guts of the operating system and has to play around with memory directly and point to different instructions in different parts of memory to get the computer to fail in a useful way. Until recently, most operating systems stored their own internal commands in known, static locations in memory. Thus the attacker could just point to those commands with his malicious instructions, and use the tools of the operating system itself to take over. Library Randomization randomly distributes those commands throughout memory every time the operating system loads. Thus, even if an attacker finds a buffer overflow vulnerability and pushes his commands onto your system, it's extremely difficult for him to turn that into a working exploit.

That's why we call Library Randomization an anti-exploitation technology - even when the bad guys find vulnerabilities (and they will) it will be much harder for them to exploit your system. This is a big move, since instead of relying on programmers to write perfect code, Apple - following the lead of Microsoft and some Unix/Linux variants - is hardening the operating system to make exploitation itself more difficult. Apple actually started down this road with Mac OS X 10.4.7 when they enabled Data Execution Protection, a feature available on some processors to let programmers mark memory locations as data only, limiting the ability of an attacker to push a command in.

I'm sure security researchers will eventually figure out a way around it, but early signs from other operating systems indicate that Library Randomization is a serious obstacle for an entire class of attacks. I've spent a lot of time on Library Randomization because, following Time Machine, it's probably the most significant security update in Leopard, but those two are far from the only improvements.

**Identifying and Defanging Evil Apps** -- As firewalls become more ubiquitous it's becoming harder for bad guys to attack computers directly over the network. Many are switching over to what we call client-side exploits - getting

malicious code onto your system via malicious email, Web pages, and file downloads. While Apple can't prevent people from downloading dangerous stuff, Leopard has a new feature to tag downloaded applications as coming off the Internet.

The first time you run a downloaded application, your Mac will ask you to approve it and tell you when it was downloaded, what application downloaded it, and where it came from. This is another great feature that should help limit malicious software from downloading and executing programs without your knowledge. The one potential weakness I see is this warning could be used to trick you into visiting a malicious Web site, and I hope Apple is taking that into account.

Apple has also added application signing. Apple, and any developer that wants to participate, can affix a digital signature to their applications. Digital signatures are valuable because they certify both where an application came from and, more importantly, that it hasn't been modified. If a bad guy tries to subvert a signed application on your system, the modified application will no longer match its signature, and Mac OS X won't allow it to launch.

Leopard's next important feature is "sandboxing." Sandboxing is a technique of restricting specific applications so they can't perform certain kinds of actions, like limiting the files they can touch, the other applications with which they can communicate, or what they can do on the network. Some applications will always be at a higher risk than others for compromise, and sandboxing helps prevent those applications from being used to take over other parts of your system. The Leopard Web site lists Bonjour, Spotlight, and Quick Look as being sandboxed. This is interesting because those are all services that look at arbitrary files or network packets, making them more vulnerable to a popular type of attack called fuzzing, where the attacker plays with input (like files and network packets) using automatic tools, looking for a data stream that will choke the recipient service. The infamous Wi-Fi hack (see the TidBITS series "[To the Maynor Born: Cache and Crash](#)") was discovered using fuzzing, as were most of the

bugs in the Month of Apple Bugs (see "[MoAB Is My Washpot](#)," 2007-02-19). I'll be curious to see the entire list of sandboxed applications, and if Safari and QuickTime are included since they are also exposed to this type of attack.

**Other Notable Improvements** -- While perhaps not as significant as the updates we've already talked about, Leopard also includes a bunch of other security improvements. The Mac OS X firewall, based on the open source ipfw program, has been improved and now includes the capability to block network access to individual applications. I've heard rumors that Apple's default firewall rules are no longer user accessible, which would be a major step backwards, but letting the firewall control individual applications is a long-desired feature for us security geeks.

The Keychain has been enhanced to manage multiple user certificates for email encryption and digital signatures better, which will be welcome for those of us with multiple email accounts. Encrypted disk images now use 256-bit keys instead of 128-bit keys (much more than twice as strong), and although I don't know anyone who can break a 128-bit key, thanks to the way AES functions, performance should be essentially unaffected.

A few changes help improve compatibility for those of us using Macs in corporate environments. Native VPN support has been updated, and Windows SMB packet signing is now available, to provide compatibility with encrypting Windows file servers. Apple also enhanced file sharing with more granular access control lists, enabling more control over who can access your shared files. (Glenn Fleishman's "[Take Control of Sharing Files in Leopard](#)" has all the details there.) While useful in any environment, I suspect some of these improvements were added to help with sharing in corporate environments and to complement the access controls in Windows environments.

Apple hid a few security features in other parts of the Leopard. One I'm really looking forward to is the guest account that purges itself entirely after the guest user logs out (for details, check out Kirk McElhearn's "[Take Control of Users & Accounts](#)

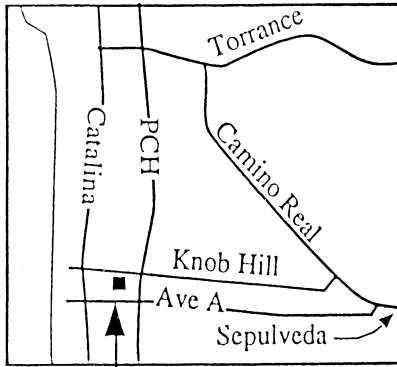
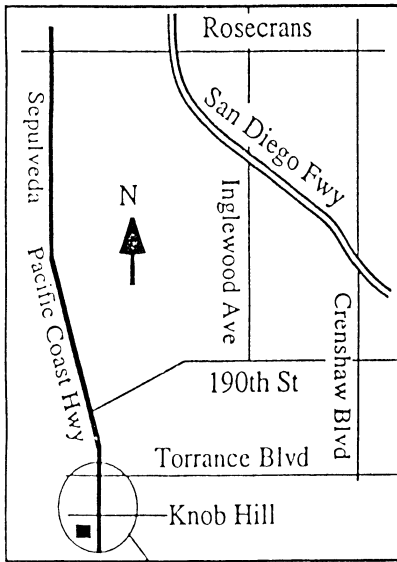
[in Leopard](#)"). While I don't let many people touch my MacBook Pro, there are occasions when I want to allow temporary access so someone can copy a file from me, check email or look something up online. A temporary guest account is a great way to enable this safely and without leaving even a trace on my Mac afterwards.

We'll also now get to see the encryption status of wireless networks right from the menu bar, so you can avoid even bothering to connect to protected networks. Those of you with kids gain improved parental controls that include Web filters, activity monitoring, and even a built-in filter for Wikipedia. Finally, with the inclusion of DTrace and a new instrumentation interface, we security geeks can really dig into the system internals and see what's going on. I expect to see more than a few security tools that take advantage of this capability.

One open question I'll be checking the moment my copy of Leopard arrives is whether Input Managers are still part of Leopard. Input Managers are a valuable feature to enhance applications, but they are also unfortunately a serious security risk (see Matt Neuburg's discussion of this in "[Are Input Managers the Work of the Devil?](#)" 2006-02-20). Apple has hinted that Input Managers might be restricted in Leopard, and despite the cries from some in the development community, I believe Input Managers need to be changed to improve our security or eliminated altogether.

Overall, Mac OS X 10.5 Leopard is perhaps the most significant update in the history of Mac OS X - perhaps in the history of Apple - from a security standpoint. It marks a shift from basing Macintosh security on hard outside walls to building more resiliency and survivability into the core operating system. We still need to see how these features hold up once security researchers get their hands on them, but the security future looks promising and I'll sleep better at night knowing my mother can still safely bank online.

*[Rich Mogull currently works as an independent security consultant and writer through [Securosis.com](#) after having spent seven years as an analyst with Gartner.]*



We're at 320 Knob Hill at  
PCH • Free Parking

## THIS MONTH'S MEETING

**Wednesday November 28th, 2007 7:30PM**

320 Knob Hill, Redondo Beach  
(see map at left for directions)

### Tony Hayes of the Apple Store Returns

In September, we learned so much from the Apple reps from the Manhattan Beach Apple Store that we asked them to return. On November 28th, Tony Hayes will be joining us again with one of his people to continue the presentation on new Apple software.

Don't miss it!

#### And Of Course:

*Come early (6:30) for Beginners Q & A Sessions! We now have two: one in the main hall hosted by Bob Brooks & Jim Pernal and the other in the kitchen area hosted by LJ Palmer*

### December 26th Meeting Details:

Bring all your questions and join us for pizza! This is the one meeting of the year to explore all those questions you've been wondering about. Our resident experts will be assembled and ready to take on the challenges you give them!

***GREAT RAFFLE PRIZES TOO, TICKETS ONLY \$1 EACH!***

### How Much Do You Benefit from the SBAMUG?

Can you help out by hosting a Core Group meeting, bringing some refreshments to the general meeting, set up, clean up, whatever! Please let us know. This is a volunteer organization and we all need to pitch in!

### INTERNET ACCESS

Don't forget we have wireless internet access at our meetings. Bring your wifi capable laptop with you when you show up for our next meeting!

Any comments or ideas for future meetings? Write it down and drop it in our Suggestion Box on the refreshment table at our monthly meetings, or speak to a Core Group member.



# PERIODICALS

**South Bay Apple Mac User Group**  
P. O. Box 432  
Redondo Beach,  
CA 90277-0432



## SBAMUG Membership Application

South Bay Apple Macintosh User Group provides Mac owners and users with a local source of shared knowledge and experience through monthly meetings, training seminars and our monthly newsletter.

Individual and family membership is \$35 per year payable to SBAMUG.

New Member       Member Renewal

Name: \_\_\_\_\_

Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

Home Phone: \_\_\_\_\_ Email Address: \_\_\_\_\_

Special Computer Interest: \_\_\_\_\_

Model of Macintosh You Use Most: \_\_\_\_\_

How did you hear about SBAMUG?: \_\_\_\_\_

Comments: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Bring Application & Fees to Meetings or Mail to:  
SBAMUG  
P.O. Box 432  
Redondo Beach, CA 90277