December 2008
Vol. XIX, No 11

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ http://www.keystonemac.com

Join us on December 16 for the annual Keystone MacCentral Holiday Party.

We will have our business meeting and Q & A period, followed by a program that will include plenty of time for eating and socializing. KeyMac will provide soda; we ask members to bring in something good to eat.

The evening's program will feature an exploration of Apple's web site, an informative video by Christopher Breen, and Jim Carey will show off his new Drobo. The safe, expandable Drobo storage solution protects your data against a hard drive crash, yet can expand dynamically at any time in just seconds. With nothing to configure or manage, Drobo is the ideal solution for primary storage as well as backup.

Meet us at

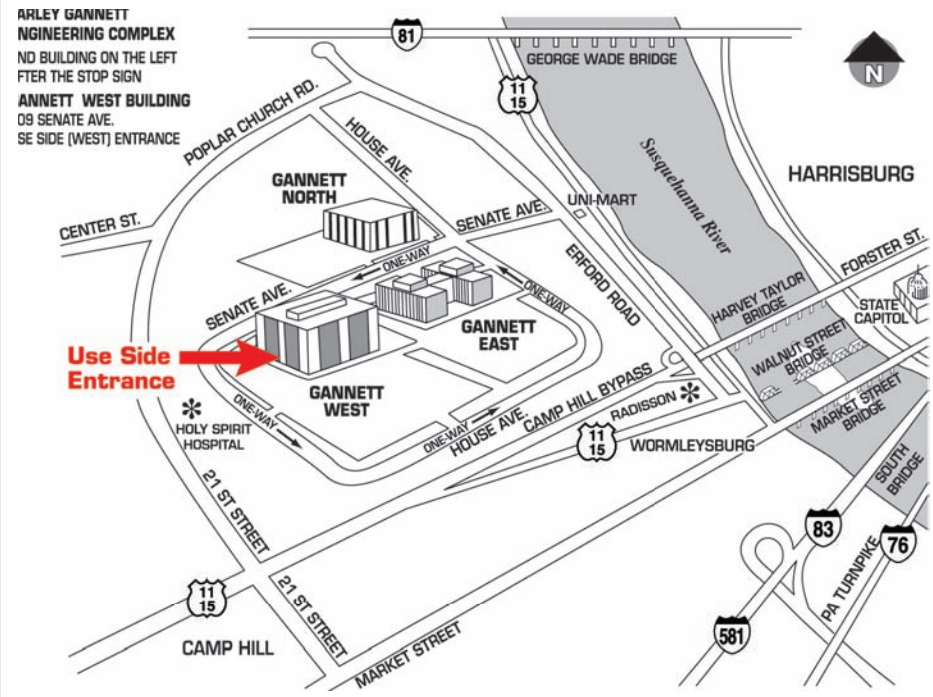
Gannett Fleming

Gannett West Building
209 Senate Ave ❖ Camp Hill

Tuesday, December 16, 2008, 6:30 p.m.

Attendance is free and open to all interested persons.

Contents



Keystone MacCentral Essentials

Meeting Place
Gannett West
209 Senate Avenue
Camp Hill

Web Site
http://www.keystonemac.com

Mailing Address
305 Somerset Drive
Shiresmanstown, PA 17011

by Linda J. Cober

President's Corner

Our December meeting should be a good one with our traditional Christmas party coupled with some informative presentations about painless new ways to backup and archive everything on your Mac from your photo and music libraries to documents. We will also explore Apple's website and show you some things you may not have been aware of thus far. As far as the party portion of the meeting is concerned, the club will provide ice, soft drinks, cups, napkins and utensils while you are asked to bring some goodies to share. If everyone contributes as usual, we will have a great assortment of foods of all types from appetizers to desserts. Jim, of course, is really hoping for some soft pretzels while I am looking forward to Wendy's delicious chili and maybe some homemade cookies. :-)

As you know, I am a teacher who embraces the use of technology, not only in groups such as ours where we strive to educate members and improve our use and enjoyment of our Macs, but also at school. My 9th and 10th grade English classes are currently using iMovie and our Mac laptops to create their midterm projects. I have been doing these projects for about four years now, and both my students and I have learned a lot in the process. I give the 9th and 10th graders different assignments since some of the 10th grade students were in my 9th grade class the previous year, and I don't want anyone to repeat the previous iMovie. Most of the students are fine with this, but some of them would really like to re-do the previous year's project with another interviewee. Thus far I have not permitted them to do this, but I am considering accepting proposals next time around because I am curious about the changes they would make in their projects if given a second chance. I know that I always see places where I could have improved my iMovies. The students who did not have me in 9th grade most likely did not do an iMovie in English, although they probably did a PowerPoint or Keynote project. I am one of the few English teachers who has students do an individual iMovie rather than having them work in groups. Working as individuals is harder because everybody has to learn iMovie, not just assign the most computer savvy group member to make the iMovie while the rest of the group members provide the information to be included. I know this occurs because back when I used to have students film their own scenes from Romeo and Juliet or Julius Caesar, I watched this division of labor take place in the groups. As a result, I now have 10th graders who don't know iMovie despite having helped create one in another class. One girl told me that she doesn't know how to use the program at all because her part in her group was to find the information while another student made the actual iMovie. She can do online research but can't use iMovie, while the reverse may be true for her group member. Our project requires those skills and more. I promised to help her learn iMovie, so she will not be in the same position next year. I used to show a tutorial to the whole class before we began, but don't take the time now because most of the students feel capable of starting their movies on their own and don't pay attention to the tutorial. They prefer to wait until they need the information and then ask me to help them personally with the problem. I actually find helping solve problems as they occur to be an effective teaching method since about half of my students made their own iMovies last year and thus are ready and willing to serve as peer tutors. For major things such as scanning family photos or adding digital audio from interviews conducted with an iPod and iTalk, I teach the first two students who need help how to do it, then they teach the next ones who request aid while I go back to helping other individuals who are having specific problems. I recently got the book *A Teacher's Guide to Digital Media in the Classroom by* Richard Harrington (who also wrote another book in the Apple Training Series called *iWork '08* which was reviewed in my October President's Corner.) Both books are published by PeachPit Press and are eligible for our KeyMac group discount as mentioned last month and also at our meetings. If you are a teacher, especially if you are just getting started or wanting to get started using technology in the classroom, you would find this book extremely helpful. One tip, which I will be sharing at our meeting as we explore Apple's website, is the availability of online tutorials at www.apple.com/ilife/tutorials and at www.apple.com/iwork/tutorials. If you decide to use these tutorials, be patient. I am on a DSL connection at home and still found the downloads to be slow, whether using Safari or Firefox. They do a good job of providing basic information, however, and allow users to choose parts of the tutorials rather than having to listen to the whole thing when there is just one area in which one needs help. I wish my PA Dept. of Ed. mandated online embedded learning course did the same thing since I find myself having to sit through segments of Project Based Learning which I could have written!

Please join us for our annual Christmas party and meeting on December 16 and bring some tasty food to share! Hope to see you there!

Now that winter and, at times, hazardous driving conditions are here, it may become necessary to cancel our meeting.

If schools, either day or evening, are cancelled, we will also cancel our meeting.

by Gary Brandt, Recorder

Keystone MacCentral Minutes

November 18, 2008

Business Meeting

President Linda Cober welcomed members to the November meeting and reminded us to bring food to share at the December meeting. KeyMac will provide the sodas. Webmaster Linda Smith posted a new application to our web site. Lock Desktop 1.2 will lock your desktop without the necessity of shutting down any applications you might have running. We have a tentative offer from someone to do a demonstration of GarageBand. We have a training DVD for that program that can serve as an introduction to the GarageBand interface.

Q&A & Comments

We talked about FIOS service and a few people gave positive comments. Channel choice might even be greater than with cable. Jim Carey mentioned a small USB device costing around $140 that works with eyeTV. You connect an antenna to the device and connect the device to your computer to receive the TV signal on your computer. Depending on your location, you might be able to pick up strong digital and analog signals.

A question was raised about viewing our newsletter PDF in Safari. There was no satisfactory way to get the page size correct. Options would be installing the Adobe Acrobat Reader plug-in or downloading the PDF to disk before opening it in Acrobat Reader or Preview.

Linda Cober wanted to know what version of Safari worked with Mac OS X 10.3.9 because an acquaintance was having problems. We looked at preference files to find any linked to Safari. Try trashing the com.apple.Safari.plist file and starting Safari to build a new preference file. If that does not help, a reinstallation from the install disk would probably be necessary. Linda mentioned using the Apple Knowledge Base to find a list of Mac keyboard commands.

Someone mentioned that they had heard TurboTax would not allow a second tax return to be filed without an additional charge next year. A member was looking for fax software to use with a Mac. Eric Adams has PageSender but he mentioned that he normally sends e-mail attachments rather than faxes. There are some free and some commercial online fax alternatives.

Jim Carey said that he can do most image correction functions on his photos using Aperture. Jim suggested that Aperture might even be superior to Photoshop for correcting RAW files.

Program Notes

We watched more of the Numbers '08 Essential Training DVD at the November meeting. We began with the section demonstrating the use of checkboxes in table cells. Checkboxes can have a default status of checked or unchecked. Other options to control input into table cells were shown. Cells can be formatted as steppers or sliders with minimum and maximum values and increments predetermined. A popup menu allows you to set and limit the numerical or text values that can be entered into a cell.

Another need when working in a spreadsheet might be monitoring cell values and applying conditional formatting based on those values. This ability in Numbers was demonstrated using the Cells Inspector. Narrator David Rivers also showed how to use the autofill features available. There is a small circle at the bottom right corner of a table cell that can be dragged down or to the right to autofill when Numbers recognizes a repeating pattern.

David showed how to reorganize tables using a sample telephone number list. Selecting any cell in a table will make the Sort & Filter button active. Sorting keeps data together in its respective rows. David demonstrated second level sorts and filtering. Sorting also works within a selected range of cells.

The next section we watched dealt with the use of formulas with either the formula bar or the formula editor. When entering a formula in Numbers, the cells you are using for that formula are highlighted. Entering the = sign as the

first character in a cell brings up the formula editor where the rest of the formula can be typed. The two types of cell references were explained. Relative cell references are used when formulas are copied and pasted. Formulas can also be set up to use absolute cell references. You put a $ sign before and after the cell location in the formula to make that cell reference absolute. You can use cells from other tables or other sheets in Numbers. The easiest way to enter cell locations is by clicking on the referenced cell when entering a formula. We did not view the section on functions, but Numbers contains the commonly used functions found in other spreadsheets.

We skipped to the section of the video about working with charts. if you add a chart to a Numbers document without having a table selected, a chart will be added with data from a sample table that is also added. Since this is not normally what you want, you need to select the table data you want to chart before adding the chart. Numbers has both 2D and 3D chart styles. The Chart Inspector is used to modify the look of charts. You can chart noncontiguous groups of cells by using the command key when making your selections.

The section on working with text in Numbers demonstrated using tabs and indents. Turn the rulers on to show and set their placement. By default in Numbers, clicking the Tab key moves the cursor five spaces to the right. To set your own tab stops, click on the ruler. Right-clicking on a tab stop in the ruler brings up a popup where right, left, center, and decimal tabs are set.

Numbers '08 integrates with Apple's Address Book data. As long as you are using a table style that has a header, you can fill that table with any fields from Address Book. The field names must be entered into the Numbers header exactly as they appear in Address Book. Once your table is set up, you open Address Book and drag either single contacts or groups onto the Numbers table and Numbers grabs the appropriate data to fill in the table cells. If you drag contacts from Address Book into a blank area of a Numbers canvas, a new table is created. By default, listings for last name, first name, phone, and email are shown in the resulting table. However, all of the information for each contact dragged over is available but hidden. You can use the Table menu to show or hide the other columns with this information.

Raffle

We held a raffle after the program. We gave away a gift certificate good for a free download from the macProVideo.com or designProVideo.com web site. The winner was Don Fortnum.

by Glenn Fleishman

Laptop Recovery Software Uses Wi-Fi and Flickr

The latest laptop-recovery application is a kind of mash-up, using several systems to provide information about a laptop's location and who's currently using it. GadgetTrak's new MacTrak ($59.95, one-time fee) uses Skyhook Wireless's Wi-Fi Positioning System, the same technology that's part of how the iPhone and iPod touch determine location. MacTrak also uses Flickr as a way to post photos snapped of someone using a machine identified as lost or stolen.

There are already several programs available that let you install software that's regularly checking for an activation signal to leap into action if your laptop is marked (in various ways) as being out of your hands. For a full rundown, see "Help! I'm Being Held Captive, and All I Have Is a Wi-Fi Network!," 2008-05-03.

But MacTrak appears to have — or at least disclose — the most accurate way to track a missing computer. Skyhook's WPS relies on being in areas that have enough Wi-Fi signals to pinpoint a location, and on having an active network over which to perform queries. It's likely that a stolen laptop would wind up on a network in a city, unless thieves are becoming savvy and keeping computers locked down.

MacTrak also uniquely transmits collected information directly to you, uploading it to Flickr (if you have an account set up, which is free for limited uploads), and sending via e-mail. GadgetTrak says they don't run a monitoring center but will help connect users with law enforcement if asked.

I'd love to see the face of a police officer, used to dealing with unrecoverable machines, when you walk in with a picture of the thief, a set of GPS coordinates with a map, and information about the network on which the thief connected.



by Tim Sullivan

Rumors and Reality

Around Apple

• There is speculation that Apple may ship Snow Leopard, the next major revision of Mac OS X, early in 2009. This rumor was fueled by what might have been a slip by an Apple employee at the Large Installation System Administration Conference, a technical conference targeted at engineers and system administrators. A slide indicated a ship date of Q1 2009.

• If you like to watch Apple commercial on TV, there are a few "unaired" commercials at <http://www.macblogz.com/2008/11/30/unaired-apple-commercials-the-definitive-list/>

• Apple has submitted a patent application to use liquid coolants to transport heat in its notebook computer designs.

The new cooling systems could extend into their other portables such as the iPhone, iPod touch or even a yet unseen gaming console. With Quad-core processors coming to market in the coming year, cooling systems are going to be paramount in keeping desktops, laptops and other devices cool.

Don Quixote or White Knight? A Harvard Law School professor, Charles Nesson who consulted on the case against chemical companies that was depicted in the film "A Civil Action," is challenging RIAA.

RIAA, the Recording Industry Association of America, takes swapping music via the internet very seriously. Few of their cases have gone to trial. Most defendants would rather settle out of court than risk have to pay overwhelming court coasts and fines.

Nesson became involved when 24-year-old Joel Tenenbaum, a graduate student, was accused by the RIAA of downloading at least seven songs and making 816 music files available for distribution on the Kazaa file-sharing network in 2004. Tenenbaum offered to settle the case for $500, but music companies rejected that, demanding $12,000.

The Digital Theft Deterrence Act, the law at issue in the case, sets damages of $750 to $30,000 for each infringement, and as much as $150,000 for a willful violation. That means Tenenbaum could be forced to pay $1 million if it is determined that his alleged actions were willful.

Nesson argues that the Digital Theft Deterrence and Copyright Damages Improvement Act of 1999 is unconstitutional because it effectively lets a private group — RIAA — carry out civil enforcement of a criminal law. He also says the music industry group abused the legal process by brandishing the prospects of lengthy and costly lawsuits in an effort to intimidate people into settling cases out of court.

Nesson believes the industry could develop new ways to prevent copyright material from being shared illegally. One idea would be to bundle music with ads and post it for free online, he says. "There are alternative ways," he said, "of packaging entertainment to return revenue to artists."

Progress marches on. Here comes USB 3. The new version will provide data transfer speeds that peak at 4.8Gbit/sec, around 10 times faster than the USB 2.0 standard and six times faster than FireWire 800. It will also provide more power to the connected devices, reducing the number of devices that need external power supplies. One downside is that USB 3 will not be compatible with USB 1 devices.

Look for USB 3 devices to start showing up in 2010.

Firewire appears to be on the ropes, but will not go down without a fight. The 1394 Trade Association is pressing on with the development of the next version of FireWire.

One advantage of Firewire is that it is more efficient, not placing heavy demands on the host computer's CPU, something that USB does.

Kill Pill: A major headache for IT departments is stolen or lost laptops full of really interesting data. It estimated that laptop thefts rose by 84 percent in 2006 compared to the prior year.

Fujitsu Siemens Computers is attempting to address this problem via a two pronged approach. The company will offer customers a security package that will allow them to locate their laptops, as well as protect confidential data, in case of theft.

Users register their laptops with the Computrace Customer Centre, and if their machines are stolen, they can report the theft, online or via telephone, in a similar manner as reporting the loss of a credit or banking card. SystemTrack then tracks the stolen machine in real-time and detects its location as soon as the device is connected to the Internet or intranet. The device can even be recovered in this way.

In the meantime, the support desk can access the system and save the confidential data centrally in the system or, if necessary, completely delete such data. It can also render the hardware useless via a so-called "kill pill." If the device is returned to the customer after the kill pill has been activated, users can remove the protection and boot the system again using a special password.

by Joe Kissell

Securing Your Disks with PGP Whole Disk Encryption

I've been using various incarnations of PGP (Pretty Good Privacy) encryption software for almost as long as I've been a Mac user. I won't go into PGP's long and interesting history (for that, see this Wikipedia entry), but since 2002, commercial Mac versions of the software have been available exclusively from PGP Corporation. PGP is commonly used for encrypting email and chat, and the PGP Desktop software can also create encrypted disk images that offer capabilities unavailable with Apple's Disk Utility.

In addition, for some time PGP Desktop has been capable of encrypting an entire disk or partition - but until recently, you could do this only for non-startup volumes. Now, however, with the release of PGP Whole Disk Encryption for Mac OS X (also included with version 9.9 of PGP Desktop Professional for Mac OS X - though not with PGP Desktop Home), that limitation has finally disappeared. It may sound like a fairly trivial change, but this is something I've been waiting for since the days of Mac OS 9, and in my opinion it's a Pretty Big Deal (PBD). I've frankly been surprised that this new capability has received so little attention, so allow me to do my small part to rectify that.

Why Encrypting a Startup Disk is Interesting — Suppose your Mac's hard disk contains sensitive information of some sort - confidential business plans, personal financial records, secret love letters, or whatever. You could put all that information on an encrypted disk image, which is plenty secure but potentially awkward to use; you must be careful not to store any private information anywhere other than that disk image, and every time you want to mount it, you must enter your password. Or you could use Apple's FileVault feature, which encrypts everything in your home folder (including your iTunes music, your iPhoto photos, and so on). That should cover most of the bases, but FileVault introduces some complications when it comes to backups (in particular, it's only partially compatible with Time Machine), and the way it stores information makes it potentially susceptible to large-scale data loss from random disk errors. In addition, FileVault must periodically perform time-consuming maintenance to free up disk space, and it doesn't protect any data stored outside your home folder.

Speaking of backups, I always recommend creating bootable duplicates of your entire startup disk - and, for extra safety, I suggest making two or more copies and keeping one offsite at all times (for example, at a friend's house). You should do this, of course, even if you have no need to encrypt your Mac's internal hard disk. But if someone happened upon that offsite backup, there'd be nothing stopping them from reading everything on the disk. Even if you'd used encrypted disk images or FileVault to protect part of the disk's data, some private information could still be at risk. Although lots of backup programs offer encryption, they invariably do so by wrapping up all the data from your disk in a special archive file or disk image, preventing the disk from being bootable. So, until recently, the only way to get bootable duplicates that were also totally encrypted was to use one of the few, and expensive, hardware-encrypted enclosures, which require a physical key to unlock your data.

Now suppose you could encrypt every last byte of data on your startup disk - any startup disk, even an external FireWire or USB bootable duplicate - all at once, without fiddling with disk images or FileVault, without any backup caveats, without any intrusive rituals to interrupt your work, and without any performance penalties. As a matter of fact, you could do just this, years ago, with any of several classic Mac programs that encrypted entire disks at the driver level. (My personal favorite was a component of FWB's Hard Disk Toolkit - may it rest in peace.) But for a variety of reasons, none of these utilities made the jump to Mac OS X. That means ten-year-old Macs (not to mention brand new Windows PCs) could do something that modern Macs couldn't do. But earlier this year, for the first time, that changed.

The first company to introduce whole-disk encryption for Mac OS X was Check Point, which released Check Point Full Disk Encryption in May 2008. I haven't yet tried Check Point's product, but then, it's not marketed or sold to individual end users; it's designed for large-scale deployment in businesses and requires non-trivial setup procedures to be performed by a system administrator. Luckily, PGP released its Whole Disk Encryption products just a few months later, and they're readily available to ordinary folks like you and me.

Incidentally, both PGP Whole Disk Encryption and Check Point Full Disk Encryption can work their magic only on Intel-based Macs. To be more precise, PGP's products can

Continued on page 8

Continued from page 7

Securing Your Disks with PGP Whole Disk Encryption

run on PowerPC- or Intel-based Macs, and can encrypt entire volumes on either variety of Mac, but encrypting a startup disk requires a Mac with an Intel processor.

How PGP Whole Disk Encryption Works — To encrypt a whole disk (whether a startup volume or not), you open PGP, select PGP Disk in the program's sidebar, and click Encrypt a Disk. The program then walks you through a few brief steps, such as selecting a passphrase, and begins encrypting the disk in the background using the AES-256 encryption standard. The process takes some time, depending on the speed of your computer, the size of the disk to be encrypted, and how much other work you're doing. In my case, it took about 10 hours to encrypt a 250 GB disk on a 2.4 GHz MacBook Pro, but I was keeping the machine extremely busy with other tasks at the time (installing Windows in a VMware Fusion virtual machine, for example). I didn't find that the encryption slowed me down unreasonably, but if I had, I could have clicked a Pause button and resumed the encryption at my convenience.

When you encrypt an entire disk, you can normally choose between a manually entered passphrase and a public key (which could, for example, let someone else decrypt the disk without your having to know their passphrase). With startup disks, you must always choose a passphrase, but after the disk is encrypted, you can grant access to more users, each of which may use either a passphrase or a public key. (To access a disk encrypted with a public key, someone would use their corresponding private key; see Wikipedia for more on how public-key cryptography works.) If the need arises, you can change the passphrase for any user after the fact without decrypting the disk; you can also re-encrypt an already encrypted disk in much less time than it would take to start from scratch.

Once your disk is encrypted, nothing special happens until you shut down or restart your computer (or, for a non-startup disk, unmount the disk). When you attempt to start up your Mac, you initially see a special PGP BootGuard Screen, where you enter your passphrase. Once you've done so, startup continues normally. (If you mount a non-startup disk while your Mac is running, you see a simple alert dialog with a field to enter the passphrase.)

After you've unlocked your Mac with your passphrase, Whole Disk Encryption is normally invisible as you use your Mac. I did not perceive any performance slowdowns in day-to-day use (even with disk-intensive activities), and for all practical purposes, everything behaved exactly as it did before.

You can mount an encrypted disk on another computer — even a Windows computer — as long as it has the appropriate version of PGP Desktop or PGP Whole Disk Encryption installed. If you've encrypted an external FireWire or USB drive containing a bootable duplicate, you'll be prompted to enter your passphrase on any Mac when you use it as a startup disk (since the disk itself contains the PGP software, it need not be installed separately on other computers). Note, though, that because Whole Disk Encryption works only on Intel-based Macs, you can't use such a drive to start up a PowerPC-based Mac.

If you were to forget your passphrase, your data would ordinarily be gone forever: this is strong encryption, and tricks like using data recovery software will be of no use. However, if (and only if) you're using PGP Whole Disk Encryption in a managed environment - meaning an administrator centrally deploys and configures the software - there is a fallback plan. Your system administrator can issue a one-time, per-device token that gives a particular user an opportunity to recover data from a single encrypted disk. (That means the administrator could also potentially get at your data, but that's to be expected in managed settings.) Individual users have no such back-door option.

Qualifications and Gotchas — As convenient and transparent as Whole Disk Encryption is, it comes with some limitations I wasn't expecting, and which gave me pause. These may or may not be issues for you, but it's important to be aware of what this software can and can't do.

First of all, although all the data on your disk is encrypted all the time, it's freely accessible from the time you turn on your Mac and enter your passphrase on the BootGuard screen until you shut down (or restart) the computer. You can't turn off access manually without shutting down or restarting. Crucially, Whole Disk Encryption does not disable access to your data when your computer goes to sleep or require entering your passphrase when it wakes up. So, suppose you've encrypted your MacBook's hard disk, but you normally put the computer to sleep when you carry it around. (Like most owners of Mac laptops, I do this to eliminate wasted time waiting for the computer to restart whenever I want to use it.) Now, the unthinkable happens and someone steals your computer. As long as the thief doesn't shut it down or restart it, the disk's encryption is useless - any data on it can be freely accessed directly, or over a network.

You can minimize the risk by choosing a strong login password and by making sure you must enter it when your Mac wakes from sleep (check Require Password to Wake This Computer from Sleep or Screen Saver in the General view of the Security pane of System Preferences), because in order to reset your password without knowing it, an

attacker would have to restart your Mac. Still, this situation bugs me because Whole Disk Encryption seems most useful for laptops, and laptops seem most useful when you employ sleep mode rather than shutting them down after each use.

Second, Whole Disk Encryption for startup volumes isn't compatible with Boot Camp, at least not in this release. If you install Whole Disk Encryption while a Boot Camp partition is present, you'll see a warning message to the effect that you can still encrypt whole disks, just not your startup volume. If you use Boot Camp Assistant to remove your Boot Camp partition, you can then encrypt your startup disk. But you have to choose between Boot Camp and having your entire disk encrypted.

Third, if your disk requires repair or troubleshooting, you're going to run into problems. For example, with an encrypted startup disk, you can't perform a Safe Boot. Holding down the Shift key while restarting normally disables some potentially problematic software, such as third-party kernel extensions, but since Whole Disk Encryption relies on such an extension to provide access to your disk, this won't work. Furthermore, you can't use disk repair programs such as Disk Utility and DiskWarrior on an encrypted disk; if you have disk problems, or suspect you might, you must first decrypt the disk and then start up from another volume (say, your Leopard Install DVD) to run disk repair software. Unfortunately, the process of decrypting a disk is quite time-consuming - for me, it took considerably longer than encrypting the disk in the first place. So you could be looking at a 24-hour period to decrypt, repair, and re-encrypt a disk - not fun.

I also encountered a couple of less-serious annoyances. The first time I restarted my computer after encrypting its disk and tried to enter my passphrase, I had a moment of panic that Whole Disk Encryption wouldn't let me in. I had chosen a 32-character passphrase, and as I typed it, the cursor in the PGP BootGuard Screen moved incrementally across the passphrase field (though without displaying bullet or asterisk characters, as is often the case). After I typed the 21st character, the cursor was all the way to the end of the field and didn't move any further as I typed the remaining characters, so I got no feedback that my input was being registered. It was, and everything was fine after I finished blindly typing the passphrase, but I didn't like the fact that feedback is registered for a maximum of 21 characters when passphrases can contain up to 255.

I had also set up Carbon Copy Cloner to duplicate my Mac's hard drive to a network volume on a daily schedule, and the first time this backup ran after I encrypted my disk, it failed. Consulting the logs, and cross-referencing them with the support material on PGP's Web site, I discovered that the problem was an invisible file called PGPWDE01, which PGP stores at the root level of any encrypted volume. This file can't ordinarily be read or written by backup software, so you must exclude it manually if your backup software complains (some backup programs, like Time Machine, already ignore the file).

Recommendations — When I first heard about Whole Disk Encryption, I allowed my excitement to get ahead of reality, and I pictured a complete solution to all my encryption problems; I had the idea that this product, by itself, would eliminate the need for all the other sorts of file encryption I'd tried. As it turns out, although it solves a couple of problems brilliantly, it's still just one piece of the puzzle. It does indeed provide virtually bulletproof data protection in cases where a computer is shut down when it falls into the wrong hands, at least if you've chosen a good passphrase and taken care to prevent anyone else from learning it. It also eliminates the need to encrypt virtual memory separately (which you can otherwise do in the Security pane of System Preferences by checking Use Secure Virtual Memory), because that happens automatically. And it makes encrypted bootable duplicates incredibly easy to create.

Nevertheless, PGP recommends continuing to use multiple layers of protection, such as encrypted disk images (whether generated by PGP Desktop or otherwise) and FileVault, depending on your needs. Part of the reason is that PGP's whole-disk protection doesn't help when your computer is running or asleep; another part is that even if a determined or clever attacker could find a way to get past one layer of encryption, getting past multiple layers is much less likely. Keeping especially sensitive information on an obscurely named disk image also makes it at least a bit harder to find in the event that someone did obtain access to a still-unlocked encrypted volume.

Obtaining PGP Whole Disk Encryption — You can buy PGP Whole Disk Encryption as a stand-alone product, which costs $119 for what PGP calls a "perpetual" license - that is, a license that lets you use the version you purchased indefinitely, but which only provides free support and updates for one year. All the capabilities of Whole Disk Encryption are also built into PGP Desktop Professional (which includes encryption for email and chat, as well as support for creating encrypted disk images). Two kinds of licenses are available for PGP Desktop Professional - the perpetual license for $199, and a subscription license, which costs $83 per year. With the subscription license, you can only use the software for as long as you have the subscription. If you haven't renewed it within 90 days after its expiration, PGP automatically decrypts all your encrypted disks (after alerting you that it's about to do so), which is a potential security risk. PGP Desktop Professional 9.9 is available in a 30-day trial version, a 30.1 MB download; no trial version of PGP Whole Disk Encryption alone is offered.

by Tim Sullivan

December Software Review

Stellarium 0.10.0a
http://www.stellarium.org/
Requires OS X 10.2 or greater. Works with PPC and Intel. Freeware

I have a passing interest in astronomy and the night sky. I like to know what evening stars are out there. And right now, when the sky is clear, there are two really bright evening stars. From many years of keeping track, I have a pretty good idea which two planets are putting on the show. But which is which? Long ago I used a program called Voyager. It fell into disuse along with OS 9. I've been searching for a replacement for several years. There were two requirements: cheap and easy to use to identify objects in the sky.

Stellarium passes on both requirements. It's free. It should prove worthwhile whatever your level of interest. I was able to name the two planets very quickly (Venus and Jupiter). That's the good news.

The bad news is that this is a beta version, i.e. being tested. The main complaint seems to be that it won't load. I did not have any problems.

The screenshot shows a view looking south (the red "S") from somewhere in New York. The program initially places the observer in France. The first thing you should do is to reset to someplace closer. As an aside, the user documentation explains how to take pictures of your favorite viewing area and move them into the screen view.

There are only a few controls located on the lower left of the screen. They are reasonably self explanatory and fun to explore. One control that is helpful is the clock on the right side of the bottom dock. It starts with the system time from your computer. It can be fast forwarded to watch the sun set, the stars come out and move across the screen.

If you like to explore (or play), try the various icons. Otherwise there is a user's guide available at

<http://internap.dl.sourceforge.net/sourceforge/stellarium/stellarium_user_guide-0.9.0-1.pdf>. It serves as a guide to the program and an introduction to astronomy.

The program offers

sky

- default catalogue of over 600,000 stars
- extra catalogues with more than 210 million stars
- asterisms and illustrations of the constellations
- constellations for eleven different cultures
- images of nebulae (full Messier catalogue)
- realistic Milky Way
- very realistic atmosphere, sunrise and sunset
- the planets and their satellites

interface

- a powerful zoom
- time control
- fisheye projection for planetarium domes
- spheric mirror projection for your own low-cost dome
- all new graphical interface and extensive keyboard control
- telescope control

visualisation

- equatorial and azimuthal grids
- star twinkling
- shooting stars
- eclipse simulation
- skinnable landscapes, now with spheric panorama projection

customisability

- add your own deep sky objects, landscapes, constellation images, scripts...

Apple Updates

Safari 3.2.1 for Leopard

November 24, 2008

System Requirements

– Any Mac running Security Update 007 and OS X 10.5.5

Safari 3.2.1 for Tiger

November 24, 2008

System Requirements

– Any Mac running Security Update 2007 and Mac OS X 10.4.11

This update includes stability improvements and is recommended for all Safari users.

iTunes 8.0.2 for Mac

November 20, 2008

System Requirements

– OS X 10.4.9 or later

iTunes 8 includes Genius, which makes playlists from songs in your library that go great together.

Genius also includes Genius sidebar, which recommends music from the iTunes Store that you don't already have.

With iTunes 8, browse your artists and albums visually with the new Grid view; download your favorite TV shows in HD quality from the iTunes Store; sync your media with iPod nano (4th generation), iPod classic (120GB), and iPod touch (2nd generation); and enjoy a stunning new music visualizer.

iTunes 8.0.2 improves stability and performance and provides a number of important bug fixes,including:

- iTunes 8 and iTunes U are now accessible with VoiceOver on your Mac.

- Addresses a quality issue creating MP3s on some computers.

- Fixes a connectivity issue with the iTunes Store when using some Internet proxies with Mac OS X. Improves accessibility with VoiceOver.

Pro Apps Updates 2008-004

November 20, 2008

System Requirements

– OS X 10.4.11 (Tiger)
– OS X 10.5.5 (Leopard)

Pro Applications Updates improve reliability for Apple's professional applications and are recommended for all users of Final Cut Studio, Final Cut Server, and Logic Studio.

Compatibility Update for QuickTime 7.5.5

November 17, 2008

System Requirements

– OS X 10.5.5
– QuickTime 7.5.

This update improves QuickTime compatibility with iChat.

MacBook, MacBook Pro Trackpad Firmware Update 1.0

November 17, 2008

System Requirements

– OS X 10.5.5
– MacBook (Late 2008)
– MacBook Pro (Late 2008)

This firmware update addresses an issue where trackpad clicks may not be recognized on MacBook (Late 2008) and MacBook Pro (Late 2008) systems.

iLife Support 8.3.1

November 11, 2008

System Requirements

— OS X 10.4.11 (Tiger Only)

Continued on page 12

Continued from page 11

December Software Review

iLife Support provides system software components shared by all iLife 08 applications. This update improves overall stability and addresses a number of other minor issues. It is recommended for all users for iLife 08.

Digital Camera Raw Compatibility Update 2.3
November 4, 2008

System Requirements
- — OS X 10.4.11
- — OS X 10.5.3 or later

This update extends RAW file compatibility for Aperture 2 and iPhoto '08 for the following cameras:
- Canon EOS 50D
- Nikon D90
- Sony DSLR-A900
- Nikon Coolpix P6000

It also addresses issues related to specific cameras and overall stability.

by Doug McLean

Netflix Starts Deploying Mac-Compatible Media Player

A few weeks ago I reported on Netflix's blog announcement that the company hoped to make its Watch Instantly feature accessible to Mac users by the end of 2008 (see "Netflix Mac Support News and More," 2008-10-08). Netflix has now backed up their claim by unveiling their new media player - based on Microsoft's Silverlight technology. While it may seem surprising that the long-awaited solution to this Mac-access problem comes by way of Microsoft, you probably won't be surprised to learn that the root of the problem lies in digital rights management (DRM) technology requirements from the studios. According to Netflix:

"Apple does not license their DRM solution to third parties, which has made this more difficult, but we are working with the studios and content owners to gain approval for other solutions. As soon as a studio-approved DRM for the Mac is available to us, whether from Apple or another source, we will move quickly to provide a movie viewer that enables you to watch movies from Netflix instantly on your Mac."

The new Netflix player will use Microsoft's PlayReady DRM - new in Silverlight 2.0 - to prevent users from doing anything but watching the content. Netflix's current player relies on a Windows-only DRM system.

For those hearing about Microsoft Silverlight for the first time, it's a technology akin to Adobe Flash in that it's embodied in a Web browser plug-in and can display animations, audio and video, and interactive applications. Silverlight was first put to the test this past summer in streaming the Beijing Olympics for NBC. The player streamed thousands of hours of live coverage with generally successful results.

Unfortunately, as Mac users attempting to watch Olympic video discovered, the new Netflix player works only on Intel-based Macs, leaving older PowerPC-based Macs in the lurch. Netflix claims that Intel-based Macs account for about three quarters of the company's current Mac-based subscribers. So while a fix for the majority of Mac users is certainly better than nothing, it's a shame for that remaining 25 percent to be denied access. It's hard to imagine that Microsoft will extend Silverlight back to PowerPC-based Macs in the future.

Although Netflix initially limited access to the beta of the new player to new subscribers, the company has since opened the beta program to anyone who wants to sign up. Have at it, but remember, since it's a beta, you shouldn't expect perfect performance out of the gate.

Share Keystone MacCentral with other MACaholics

Name _____

Address _____

City _____ State ___ Zip _____

Home Phone _____ Day Phone _____

E-mail Address _____

Date _____ Is this ❍ Renewal or ❍ New?

How did you hear about us? _____

Dues for one person are ❍ $20/yr. Family or Corporate dues are ❍ $30/yr.

To join Keystone MacCentral, mail this form with your membership dues (payable to Keystone MacCentral) to:

Keystone MacCentral
Membership Chair
305 Somerset Drive
Shiresmanstown, PA 17011

Keystone MacCentral meetings are held at 6:30 p.m. on the 3rd Tuesday of the month at Gannett Fleming, 209 Senate Avenue, Camp Hill.