September 2011

mini'app'les newsletter
the minnesota apple computer users' group, inc.

Website: http://www.miniapples.org Forums: http://miniapples.7.forumer.com Email: miniapples@mac.com

From the Editor:

The biggest news in the Apple World is the resignation of Steve Jobs and his replacement with Tim Cook, the current COO of Apple. The latest news for the club is the mini'app'les Meeting on 29 September that will be showcasing Lion and iOS. Lion already has had its first update and I haven't even installed it on my MacBook Pro. Of course I had to install a larger internal drive to do that. Replacement was easy but somewhat involved but the instruction videos from Other World Computing were very clear and helpful. And it works well! Now to install Lion.

Tom Ostertag, Publications Director

Meeting Calendar

There is only one scheduled meeting for September 2011. The mini'app'les meeting being held replaces the Mac Apps SIG, the Mac OSX SIG, the iOS SIG, and the Q&A SIG for the month of September. This information was compiled as this newsletter was being assembled and is subject to change. As always, confirm the Special Interest Group (SIG) date, time, and location with the SIG Leader or the mini'app'les website: www.miniapples.org.

Meeting Calendar – September 2011			
Wednesday	September 14	7:00 pm	VectorWorks SIG*
Thursday	September 15	7:00 am	Mac Consultants SIG
Thursday	September 22	6:30 pm	FileMaker Pro SIG
Thursday	September 29	7:00 pm	mini'app'les meeting

Meeting Locations and Leaders		
Meeting	**Location**	**Leader**
VectorWorks SIG*	CJR Office, 4441 Claremore Dr., Edina	Charles Radloff, 952-941-1667
Mac Consultants SIG	Good Day Cafe, 5410 Wayzata Blvd., Golden Valley	Bob Demeules 763-559-1124
FileMaker Pro SIG	Erik's Bike Shop Corporate, 9201 Penn Ave S. #1, Bloomington	Steve Wilmes, 651-458-1513
mini'app'les meeting	Hack Factory, 3119 E. 26th Street, Minneapolis	Tim Drenk, 952-479-0891
* This SIG is NOT sponsored by mini'app'les; the listing is provided as a service to members.		

TABLE OF CONTENTS

Special Announcement Reprise

by Tim Drenk

On September 29th, mini'app'les will host a general meeting, the mini'app'les meeting, for all members. The focus will be a series of mini-presentations on Mac, Mac OS X Lion, and iOS followed by a general Mac/iOS Q&A session. We will also spend a few minutes discussing some upcoming changes to the mini'app'les website. To lighten the load on your schedule and encourage participation of all members, the Mac OS X SIG, the Mac Apps SIG, the iOS SIG, and the Mac Q&A SIG will not meet in September. (The Filemaker and VectorWorks SIGs will meet according to their published schedules.)

We want to make general meetings an ongoing event (2-4 times/year). Our hope is that this will promote a greater sense of community and allow us to present topics of general interest to a larger audience. In turn, a larger audience will attract presentations from a wider variety of developers and vendors. As the general meetings attract new members, we want them to find a SIG that interests them as well.

The general meeting, like all of our SIG meetings, is open to the public and you should encourage friends and colleagues to attend. It would be great to see some new faces amongst old friends and we'd love to "pack the house" for the inaugural event.

The topics haven't been finalized yet so if you have a suggestion, or better yet, you want to give a 15-20 minute presentation yourself, please contact Tim (timdrenk@miniapples.org) or Jeff (jeff@purpleshark.com).

mini'app'les Directors Meeting Minutes for August 15, 2011

by Joel Gerdeen

In attendance: Tim Drenk, Joel Gerdeen, Bob Demeules, Kevin Strysik, Jeff Berg, Bruce Thompson

Absent: Tom Ostertag, Les Anderson

Other Attendees: None

Agenda: See Directors' Reports and Old and New Business below.

Minutes: The minutes for the June 13, 2010, BOD meeting were approved electronically and published on forumer.com by Joel Gerdeen on June 20.

Directors' Reports

Treasurer Bob Demueles report: A written report was presented. All bills are paid. Balance in checking is $641.60. Assets $14,070. Looking at CD for higher interest rate.

President Tim Drenk report: Will check on extending domain registration for a year.

Vice President Jeff Berg report: Jeff has been working on the September Main meeting and communications that are discussed further below.

Secretary Joel Gerdeen's report: Published last report on June 20.

Publications Director Tom Ostertag's report: Good job with newsletter.

SIG Director Kevin Strysik's report: Q&A SIG dates changed. Make sure to communicate changes with Kevin, who will coordinate with others. Discussed email using address info@miniapples.org to forward to others.

Membership Director Les Anderson's report: Three members renewed over the last two months.

Past President Bruce Thompson's report: None

Old Business

mini'app'les meeting - Meeting is planned for Sept 29, 7 - 9 pm, at the Hack Factory, 3119 E. 26th Street, Minneapolis. Jeff Berg is a member there and is handling most of the arrangements. Note that during Sept, these SIGs (OSX, iOS, Mac Apps & Q&A) will not meet separately though the Filemaker and VectorWorks SIGs will meet as normal.

A tentative agenda includes an Intro by Tim Drenk, an overview of planned changes in the web site and club communications by Jeff, and three lightning round presentations of 15 min each. Afterwards, the SIG leaders will be available for answering questions about their SIGs. Jeff will guide a tour of the building for those interested. mini'app'les will provide a donation for use of the space and coffee and snacks will be provided. Jeff will be there at 5pm for setup and would appreciate some volunteers to help. Help would also be appreciated after the meeting. The Twin Cities Meetup Groups may be used to promote the meeting.

Web Page and Communications - Jeff has also been working on group communications and discussed the need for distribution list to all members with possibly an Opt-in list for SIGs for special interest. The web site needs updating possibly with a moderated blog such as Joomla, WordPress, or Drupal. The current Forumer site will be revisited and possibly dropped.

New Business

MobileMe demise - More discussion and planning is required as we learn more about Apple's move from MobileMe to the iCloud in regards to our communication planning discussed above.

Next meeting: Scheduled for October 10, 2011 at the Southdale Library at 7:00 pm. All club members are welcome to attend.

The meeting ended at 8:30 pm.

---

iOS SIG Meeting • 9 August 2011

by Joel Gerdeen

An iOS SIG meeting was held at 7 pm on Tuesday, August 9, at the Southdale Library. This SIG focuses on iOS devices such as iPhones, iPads, and iPod Touches. We discussed iOS 5 from a hands on experience with beta code though most of the information discussed can be found on Apple's web site, www.apple.com. No formal presentation in Keynote format was prepared this month.

The next meeting is planned for Tuesday, October 11 at 7:00 PM at the Southdale Library Public Conference meeting room. The meeting will continue discussion of iOS 5 and iCloud, hopefully from actual released versions. As usual, any interesting apps released during the month will also be presented. For those interested, the meeting will continue at Bakers Square afterwards.

Lion Security: Building on the iOS Foundation

by Rich Mogull

It has long been a truism among tech pundits that Apple users suffer few security attacks due to relatively low market penetration making Macs uninteresting to professional cybercriminals. That may have been true five to ten years ago, but thanks to the iPhone, iPad, and iPod touch, we can now say with assurance that obscurity is no longer Apple's primary defense against attacks.

With over 220 million iOS devices sold, Apple dominates the tablet market and is one of the major players in the smartphone market, placing the company on the front lines of the security wars. Since the initial release of the iPhone, Apple has continually added to iOS important security defenses lacking in Mac OS X to keep up with both attacks and jailbreaks. (Every jailbreak is technically a security attack used to circumvent Apple's iOS restrictions.)

How does this relate to Lion? Before Apple formalized the name as "iPhone OS" and then "iOS," the operating system on Apple's handheld devices was simply "OS X" or sometimes "OS X for iPhone." Apple representatives made the distinct point that it was merely a variant of Mac OS X, and this was reinforced once people started jailbreaking (and later developing for) the platform. While not identical, iOS and Mac OS X are more alike than different.

Apple has been extremely clear that a key goal in Mac OS X 10.7 Lion was to incorporate lessons learned on iOS back into Mac OS X. While many of these changes were focused on the user experience — gestures, Launchpad, and so on — Apple also migrated significant under-the-hood security improvements from iOS into Lion.

With Lion, Apple has focused on three significant security improvements that have been put to the test in iOS and closed one longstanding gap in how memory is protected, along with some smaller changes.

To be clear, all of these features existed in Mac OS X before Lion in one form or another; the way Apple has combined and enhanced them to change the entire Mac application and OS ecosystem clearly shows the influence of iOS.

Hardened Memory -- As I discussed in my review of the security aspects of 10.6 Snow Leopard ("Peering Inside Snow Leopard Security," 27 August 2009), Apple failed to implement ASLR completely. ASLR, which stands for Address Space Layout Randomization and is called Library Randomization by Apple, is a powerful security control that, when used in concert with other memory protection technologies like Data Execution Protection, makes it much harder for an attacker to compromise the operating system.

To review quickly, ASLR randomizes the memory locations of operating system and application components. This slows or stops attackers because even if they use a buffer overflow (or other memory corruption vulnerability) there are no known locations to hook into and exploit. It's kind of like a burglar crawling through an open window without knowing whether it opens into a bedroom or a sewage tunnel.

In Snow Leopard, Apple's ASLR implementation failed to randomize all operating system pieces, especially the important dynamic loader process, giving attackers a solid location from which to launch exploits. Lion addresses this failing, and adds other memory protections to make exploitation quite a bit harder. (This is the one area where Lion is ahead of iOS, which is still improving its ASLR).

ASLR isn't perfect, though. Many applications still use static memory locations, and if an application isn't compiled as a "position independent executable" (PIE), it, as opposed to the operating system, can be the target of the exploitation. Attacking non-ASLR applications on an ASLR-

enabled operating system is a serious source of exploits on operating systems like Windows 7 that have used full ASLR for years. On the upside, compiling an application as a PIE is the default in Apple's Xcode development environment for 64-bit executables targeted to Lion. Since Lion is available only for 64-bit hardware (which includes additional security protections that are supported by Lion too), it's now much harder to exploit Macs via memory corruption attacks.

Sandboxing and Privilege Separation -- Mac OS X has long supported sandboxing — optional mechanisms in the operating system that restrict what an application can do on your system. In recent years, Apple even used sandboxing to better protect some of their more vulnerable applications, like QuickTime. (Video players are notoriously difficult to secure due to all the different encoding methods they need to support and their high performance requirements.) Sandboxing in Lion is improved in two major ways, both of which we first saw in iOS.

First are many under-the-hood improvements in sandboxing and much more robust support for applications. Lion supports over two dozen "entitlements," which are the things an application is allowed to do. Entitlements include functions like writing to the file system (including different entitlements for temporary files), accessing the network, and interacting with hardware like the camera and USB connections. To make this work, developers design and compile their applications for sandboxing and give either an entire application, or different subprocesses, only the minimally required entitlements to work. Should an attacker exploit an application, they are thus restricted to the entitlements that application has, unless they can in some way break out of the sandbox.

Ideally, developers break their applications into separate processes, with major components sandboxed to use only minimal entitlements. Called "privilege separation," this approach provides security controls inside an application. For example, reading PDF files, rendering Web pages, viewing videos, and using browser plug-ins like Flash are all notorious sources of bugs and vulnerabilities. Apple has separated and sandboxed the rendering processes from the core applications for Safari, QuickTime, Preview, and all Safari plug-ins (back with Snow Leopard). Adobe has already sandboxed the Acrobat and Reader applications on Windows, although they haven't announced plans to do the same for the Mac OS X versions.

In QuickTime, when viewing a video file, the rendering engine is sandboxed and restricted from writing files. So an attacker who exploits QuickTime would also need to find a way to break out of the sandbox before they could, for example, install malware on your hard disk.

Applications on iOS are heavily sandboxed, but a quick check on my Lion system shows that not a single application I'm running, other than those provided by Apple, uses sandboxing. Even Apple's own Aperture isn't sandboxed.

This will all change in November 2011 when Apple implements the second major change to sandboxing and requires it for all Mac App Store apps. We don't know how carefully Apple will review individual sandboxing implementations, but at a minimum all apps submitted to the Mac App Store starting in November will have to enable sandboxing and will be less useful as a launch point for attacks. These sandboxed applications will be able to interact with your Mac only through entitlements.

Developers aren't universally thrilled with this change. Sandboxing is intrusive, and can be difficult to implement on existing code. It will even be impossible to sandbox certain applications that require features for which Apple has not yet designed entitlements. Those applications will still run on Lion, but Apple won't allow them to be distributed through the Mac App Store, and that in turn may negatively affect sales, given the Mac App Store's rapidly growing popularity as the source for Mac software.

Code (Application) Signing -- A software publisher can digitally sign an application using cryptography to assure the operating system that the application hasn't been changed, and that it comes from a

"trusted" source. A digital signature isn't merely a few bits added to the end of an application saying "I made this"; it creates a secure cryptographic hash of the entire application binary that the operating system can use to detect tampering.

Thus an attacker can't modify a signed application without breaking the chain of trust for its digital certificates — which means Mac OS X would refuse to launch the tampered application. To upload a compromised application to the Mac App Store, an attacker would need to sign their compromised version with the publisher's private key and resubmit the "update" to Apple for approval (which would of course be withheld).

Application signing has been used since 10.5 Leopard, on an optional basis, for a mix of security and usability functions. For example, certain permissions (like accessing the keychain) are managed on a per-application level. Once an application is granted access to a keychain item, Mac OS X records its signature for future access to that same item. If the application is upgraded but signed with the same signature, the keychain does not need to prompt again to allow access from the new version. In Leopard, application signing played a similar role in managing per-application firewall privileges.

Code signing is mandatory for all Mac App Store apps, just as it is for all iOS apps. However, unlike iOS, there is no system-wide requirement for code signing. But code signing does assure users that apps from the Mac App Store haven't been tampered with. The key here is not that code signing is new, but that, thanks to the Mac App Store, developers have significant incentive to implement it, and the more apps that do, the fewer can be exploited through modification.

Apple is also now using code signing more extensively for its own applications and operating system components, and it has enhanced code signing in Lion to tie it more tightly to sandboxing. Developers now have more flexibility in how they sign their code and different code components, and how those tie into sandboxing.

FileVault 2 -- FileVault is another longstanding feature of Mac OS X, but probably the one where we see the most dramatic changes with Lion. Previously FileVault would encrypt your home directory, thus protecting any sensitive files and other personal information. Combined with another feature that also encrypted virtual memory, FileVault offered reasonable protection.

But that protection came at a cost. FileVault encrypted home directories by converting them to encrypted sparse image (and later, sparse bundle) files. Each encrypted home directory was thus stored on disk as a single large encrypted file, and was highly prone to corruption. This approach also broke many backup applications, or forced them to use ugly workarounds. For example, Time Machine could back up encrypted home directories only when the owner was logged out.

Many users turned to third-party products to close this gap, but there weren't many on the market, and some (especially PGP; see "PGP Whole Disk Encryption and PGP Desktop Professional 10.0," 14 May 2010) had a habit of breaking with even incremental operating system updates. Contrast this to iOS, where full-device encryption has been standard since the iPhone 3GS, albeit with a few implementation flaws.

Whole-drive encryption won't stop a network attacker, but it protects your data in case of physical loss of your drive. I recommend full device encryption for anything mobile to all my enterprise clients, but options for consumers on Macs have been pretty limited.

This situation changes completely with FileVault 2. The only thing FileVault 2 seems to share with its predecessor is a name, and use of the word "encryption."

FileVault 2 now encrypts your entire boot disk completely transparently. You choose which users are allowed to unlock it, and only those users can boot the computer. It's fast (unnoticeable to me), works in the background (even the initial encryption, unlike the original FileVault, which would lock your system for hours if you had a lot of files in your

home directory), and works well with all backup tools.

Aside from your boot drive, you can now partition and encrypt new drives with Disk Utility. And, best of all, Time Machine even includes a checkbox to encrypt your backups.

You still need to be extremely careful with FileVault 2; if you forget your password, you are locked out of your drive forever. When you initially encrypt your system, Apple gives you two recovery options based on a 24-character code. You can write it down and use it as a recovery password, and you can store it with Apple and recover it via AppleCare after answering three user-defined security questions.

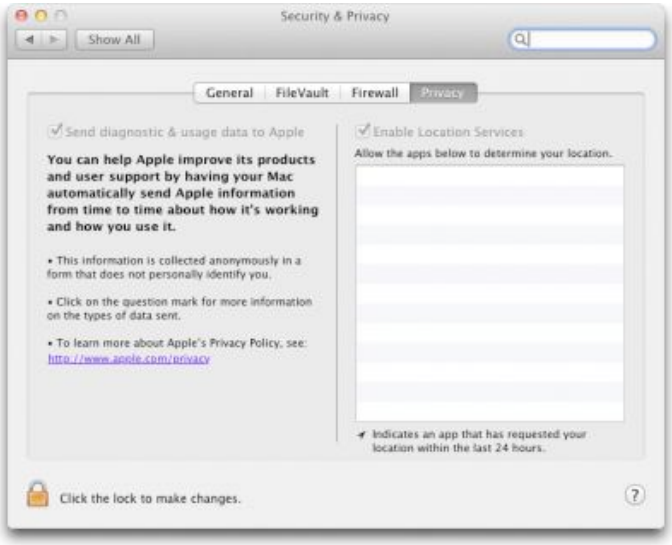
Encryption is also important for remote system wiping, one of the key security features of iOS accessed via Find My iPhone. Instead of having to format the entire drive, you just have to delete the encryption key. According to leaked information, a Find My Mac service is in developer beta and includes a remote wipe option.

Improving the Ecosystem, Not Just the System -- As I mentioned earlier, none of these changes is necessarily new to Mac OS X, and some predate iOS. Developers have long been able to sandbox and code sign their applications independently, ASLR is stronger in Lion than the current version of iOS, and FileVault 2 is a major change from FileVault, but, again, stronger than its iOS sibling.

I've also glossed over a number of other changes, including the XProtect anti-malware checks recently added to Snow Leopard ("Apple Responds to Increasingly Serious MacDefender Situation," 25 May 2011), which appear unchanged in Lion, and an additional Privacy screen in the Security & Privacy preference pane that lets you control what information your Mac sends to Apple and your location services preferences.

But it's when we take a step back that the pieces fall together and show how Apple is building security into the entire ecosystem, much as it did in iOS.

The most profound change is the combination of memory protection, sandboxing, and code signing updates with the Mac App Store. While users can still install whatever they want on their Macs, those who choose software from the Mac App Store will know (or at least benefit from the fact) that their applications enforce a security baseline that's currently rare in even major packaged applications. Compromising applications is a major vector of attack. Almost all of the recent major attacks against users (as opposed to business applications) I'm aware of rely on flaws in applications like Safari, Microsoft Excel, QuickTime, and Adobe Reader.



While I don't see Apple forcing all Mac users to use only the Mac App Store, I could see a future — either a system preference or even a special Mac — where some users are restricted in this fashion. Those users would be protected from malicious downloads and other tricks used to install malware. It wouldn't work for everyone (me, for example, or any developer), but the popularity of iOS devices and the iOS App Store proves there is a very large user base that can be more than satisfied choosing applications from a walled garden.

Remember the recent MacDefender attack, which tricked users into installing a malicious application? Imagine if instead of just asking for an administrator password, a dialog informed the user that a new application was not approved by the Mac App Store, and directed them to System Preferences to override the block. Some people would still fall for it, but over time, as users are trained to focus on the Mac

App Store for trusted applications, I bet the numbers would be far lower.

Some enterprises already do something similar with special "whitelisting" tools to restrict what employees can install, thus preventing malware. This strategy can be highly effective, albeit often hard to manage, depending on the habits of those employees and how strictly the rules are enforced.

Let's be clear about Apple's motivations here. This is clearly a case where Apple will profit from security since they get a share of every application sold in the Mac App Store. But, as someone who had to spend part of a recent weekend cleaning a relative's Windows-based PC of malware, I don't care that much as long as it works for users who are otherwise at risk.

The changes in FileVault 2, and the impending Find My Mac, show that Apple also recognizes the demand for better security on mobile computers. Apple has sold many more laptops than desktops in recent years, and this trend has continued even after the release of the wildly popular iPad. Although the combination of encryption and remote wiping has long been an option for enterprise users, Lion is the first time we've ever seen it built into a consumer operating system (even Microsoft's BitLocker full-drive encryption is an option only in its Ultimate and Enterprise versions).

In the end, Lion is significantly more secure than Snow Leopard even without the Mac App Store ecosystem. Combine the two, and we can see a future where we have security options never before available to consumers, and, more important, where security is an integral part of the overall ecosystem such that even those who know nothing about security are well protected.

Although you must take many factors into account when deciding when to upgrade to a new version of Mac OS X, from a security standpoint, the sooner you upgrade to Lion, the sooner you can benefit from Apple's security improvements.

TidBITS Watchlist: Notable Software Updates

by TidBITS Staff

Firefox 6.0 -- That's right, Mozilla has artificially jacked up Firefox's version number again, and, with the release of Firefox 6.0, as with the release of Firefox 5.0, not much has changed. Along with some stability- and security-related fixes, Firefox 6.0 sports a slightly sleeker look for the site identity block (to the left of the page URL in the address bar). Plus, in the latest episode of "Bug or Feature?" Firefox 6.0's address bar now grays out everything but the domain name of the currently loaded page, making it harder to read. Also new is an interactive JavaScript prototyping environment for developers: choose Tools > Web Developer > Scratchpad (the Web Developer menu item is also new; it collects several development-related commands). Mozilla also claims to have improved the discoverability of Firefox Sync, the usability of the Web Console, and browser startup time when using the tab-grouping feature Panorama. Apart from the silly change to the address bar, there's nothing really wrong with Firefox 6.0, as long as you think of it as version 4.2. (Free, 28.1 MB, release notes)

Dropbox 1.1.40 -- Online storage service Dropbox has updated its eponymous client software to Dropbox 1.1.40, bringing back to Mac OS X 10.7 Lion status badges on Dropbox-managed files and folders so you can tell whether or not they're updated. It also fixes a rare problem where certain Mac OS X machines wouldn't upload files automatically. In theory, Dropbox is supposed to update itself, but it often doesn't, in our experience, so it's worth getting this update manually if you're using Lion. (Free, 17.6 MB)

GraphicConverter X 7.3.1 -- Although Lemkesoft's GraphicConverter X 7.3.1 received a only minor version bump, the update comes with a large number of enhancements, including new options for manipulating images and previews, improved drawing functions, and the capability to display GPS location data embedded in image files. Support for

Mac OS X 10.7 Lion has also been improved with the reintroduction of support for the operating system's full-screen mode. Several smaller bug fixes and feature tweaks round out the update. ($39.95 new from Lemkesoft or from the Mac App Store, free update, 100 MB, release notes)

Carbon Copy Cloner 3.4.2 -- Bombich Software has released Carbon Copy Cloner 3.4.2; despite the minor version hop, this release includes dozens of bug fixes that affect several areas of the backup utility's functionality, including scheduling, the handling of network filesystems, access permission management, and so on. In at least one case, the fixes address issues that could cause a restored volume to be un-bootable under some circumstances. A number of minor feature tweaks round out the update. (Free update, 5.2 MB, release notes)

ScreenFlow 3.0 -- New from Telestream is ScreenFlow 3.0, a major upgrade to the company's screencast recording app. The new release brings a number of new features, including compatibility with Mac OS X 10.7 Lion. ScreenFlow now allows users to create freehand callouts and annotations anywhere on a video using a brush or rectangle tool. The app's timeline has received a facelift that provides additional flexibility in editing operations and is complemented by new audio quality controls and filters. Rounding out the update are new export settings, which now include an iPad preset and an option to publish to Vimeo. ($99 new, $29 upgrade, 14.5 MB)

Airfoil 4.5.5 -- Rogue Amoeba has released Airfoil 4.5.5, a minor update to its popular remote audio transmission app. The main focus of the new version is the correction of several issues related to Mac OS X 10.7 Lion, one of which is a severe crash. In addition, Airfoil now sports improved compatibility with Google Talk, Muse Controllers, and Radium (although the latter requires an as-yet-unreleased version of the Internet radio player app). ($25 new, free update, 11.3 MB, release notes)

Mactracker 6.1 -- Canadian developer Ian Page has released a new build of Mactracker, his popular encyclopedia of Apple products. Mac OS X 10.7 Lion makes its debut in Mactracker 6.1's database, alongside the latest MacBook Air, Mac mini, AirPort Extreme, and Thunderbolt Display. The update also includes bug fixes that affect areas of functionality ranging from printing to smart categories. (Free from Ian Page's Web site or the Mac App Store, 21.6 MB, release notes)

Lion Recovery Disk Assistant Creates External Recovery Drives

by Adam C. Engst

One of the initial criticisms leveled against Mac OS X 10.7 Lion was that, because it's currently available only from the Mac App Store (a $69 USB drive version is slated to become available this month), it's not obvious how to recover from problems if your boot hard disk or solid-state drive is damaged. In most situations, where your boot drive is sufficiently functional, you can still perform various recovery actions thanks to a special hidden partition called Recovery HD. In case of trouble, either hold down Command-R at startup, or hold down the Option key at boot to select and start up from that partition. The Recovery HD partition may be read-only and small — only about 650 MB — but its tools can be extremely helpful (thanks to Joe Kissell's "Take Control of Upgrading to Lion" for these details).

Once your Mac has booted into Recovery mode, you have seven possible actions, the first four of which appear in a Mac OS X Utilities window, and the remaining three of which are available from the Utilities menu:

- Restore from a Time Machine Backup. As you would expect, this option enables you to restore from a Time Machine backup on another mounted disk.
- Reinstall Mac OS X. How could you reinstall Mac OS X — which is a 3.76 GB download — from a disk that's only 650 MB in size? Simple — this option downloads the Lion installer from

the Mac App Store again. Make sure you have a fast Internet connection.

- Get Help Online. Sometimes you just need to look something up, and this option launches Safari to display some local help files. If you have an Internet connection, you can search the Web in general as well.
- Disk Utility. This option runs Disk Utility, so you can repair the disk having problems.
- Firmware Password Utility. Use this utility to set, change, or remove a firmware password from your Mac.
- Network Utility. With Network Utility, you can troubleshoot network connections.
- Terminal. Sometimes it's comforting (or at least useful) to have access to the full Unix command line.

(For a lot more interesting information about Lion Recovery, see Apple's technical article "About Lion Recovery.")

But back to my original point — what do you do if your boot drive is sufficiently damaged or otherwise dysfunctional that you can't boot into Recovery mode? Apple has now released the Lion Recovery Disk Assistant, a standalone app that you can use to make an external Lion Recovery drive using the contents of your existing Recovery HD partition. You must do this on a Mac running Lion, and if your Mac came with Lion pre-installed, the external Lion Recovery drive will boot only that model of Mac; if you upgraded from 10.6 Snow Leopard, the external Lion Recovery drive will boot any Mac upgraded from Snow Leopard. Luckily, because the Recovery HD partition is so small, you can use any external drive that's at least 1 GB in size, a perfect use for some old USB thumb drive you may have lying around. Just make sure it doesn't contain any useful data, since it will be erased in the process.

To make your external Lion Recovery drive, follow these steps:

1. Download the Lion Recovery Disk Assistant (1.07 MB) from the Apple Support Downloads site (it doesn't appear in Software Update and I somewhat doubt it ever will).
2. Connect the external drive and launch the Lion Recovery Disk Assistant.

3. Select the drive and click Continue to start the process of copying the data from the Recovery HD partition. This will take a few minutes.

4. When finished, the installer tells you how to use the external Lion Recovery drive (hold down the Option key at boot to select the drive). Note that you won't be able to see anything on this drive; the partition doesn't even appear in Disk Utility.

The process was simple and easily accomplished, and when I tested my external Lion Recovery drive, it worked perfectly. Although I don't expect most Mac users to understand the utility of such a tool, I strongly encourage all TidBITS readers running Lion to create one of these external Lion Recovery drives for Macs upgraded from Snow Leopard. And, if you get a new Mac with Lion pre-installed, create another one for that Mac. The simple fact is that you can never anticipate what will go wrong, and if Murphy has anything to say about it, the first time something goes wrong it will be sufficiently bad to prevent you from using your boot drive's Recovery HD partition.

One final note. A different way to obtain a bootable Lion recovery volume is to clone the disk image hidden inside the Lion installer onto a DVD, thumb drive, or other volume (as Joe discusses in "Take Control of Upgrading to Lion"). Doing so is a bit trickier than using the Lion Recovery Disk Assistant and requires more space (4 GB or more). But you end up with a bootable volume that has all the capabilities of the Lion Recovery drive, plus a complete copy of the Lion installer — meaning you won't need to download it again if you ever need to reinstall Lion.

Recent Highlights from the Apple User Group Resources website:

http://appleusergroupresources.com

- LAFCPUG: Fourth Annual Amsterdam SuperMeet
- Worldwide Photowalk: Terry's Team Will Walk in October
- Saudi Apple User Group: Sharing Community
- MCE Reminder: Save the Date
- Philadelphia PowerBook Users Group: Summer Festival
- DVMUG and RMUG: August 16 Film Fest
- Offers for User Group Leaders and Members including:

• Special Offer – Texting Dots Touch Screen Pads: 20% Discount
• Special Offer – IDAPT Universal Chargers: 20% Discount
• Special Offer – The Innovative Audioglove: 50% Off Clearance Sale
• Special Offer – Hand-e-holder for iPad: 20% Discount
• Special Offer – Dolly Drive: 20% Off the Time Machine in the Cloud
• Special Offer for Leaders – The Fadigear Audioglove: Demonstration Offer

http://appleusergroupresources.com/?page_id=653

The current password for vendor offers and a cut-and-paste version for newsletter editors is:

ugvendor

DealBITS

by Adam C. Engst

DealBITS is back! You may not have noticed its absence, but we did, since I had built DealBITS in Web Crossing, running on our now-defunct PowerPC G4-based Xserve. As such, moving DealBITS to our current virtual server required completely rewriting the code that manages drawings, accepts entries, and chooses winners. That's now done, and we're pleased to welcome our friends at Smile for the maiden voyage of the new DealBITS system. Of course, we're hoping everything works smoothly, but please bear with us if there are quirks or previously undiscovered rough edges.

Finally, I want to call out some minor changes in the way we're running DealBITS now.

- If you have a TidBITS account — which you do if you receive TidBITS via email or have ever bought a Take Control book from us — and are logged in (click My Account in the left nav bar of the TidBITS site), you can now enter DealBITS drawings without entering your name and email address. If you're not logged in, you'll have to enter that information, and if you don't have an account

at all, you can make one simultaneously with your entry.

- Our new system no longer tracks referrals, so while we're happy if you tell a friend about this DealBITS drawing, you won't win a copy as well if your friend is chosen as a winner. The referrals were too small of a percentage of the overall entries to make it worth coding them into the new system.
- You will no longer receive email confirmation of your entry. It seemed like an unnecessary addition to the world's email stream.

Hot Links Of The Month:
Compiled by Tom Ostertag

Apple, Inc.

Thank You, Steve Jobs. We Wish You Well. [Open Letter] | *Cult of Mac*

Steve Jobs Resigns As CEO Of Apple, Names COO Tim Cook His Successor [Breaking] | *Cult of Mac*

Apple's 'spaceship' campus larger than Pentagon, Empire State Building | *AppleInsider*

The Steve Jobs Resignation FAQ | *TidBITS*

News: Steve Jobs Resigns: The Apple Accessory Industry Reacts | *iLounge*

Mac Software

Configure The Finder Sidebar And See More In Lion [OS X Tips] | *Cult of Mac*

Mac OS X 10.7.1 Update Goes Live in the Mac App Store | *Cult of Mac*

Restore Missing OS X Features On New Macs [Video How-To] | *Cult Of Mac*

This Digital Toolbox Lets You Fix All The Little Things In OS X Lion That Annoy You | *Cult of Mac*

Subtle Irritations in Lion | *TidBITS*

10.7: Cleaning up birthdays in iCal | *Mac OSX Hints*

Apple updates Boot Camp 3.3, iMac firmware | *AppleInsider*

Mac Hardware

Apple Issues iMac Graphics Update To Correct Freezing Bug In Lion | *Cult Of Mac*

10.7: Restore Apple Hardware Test Boot Mode | *Mac OSX Hints*

iPad/iPod/iPhone/iTunes

A Sprint iPhone Will 'Drive Growth' for Apple Products [Report] | *Cult of Mac*

Tip of the Day: Scrolling inside boxes in Safari | *iLounge*

Apple issues iTunes 10.4.1 performance and stability update | *AppleInsider*

Evernote for iOS Gets A Great Update: New iPad Interface, Shared Notebooks and Rich Text Support | *Cult of Mac*

Miscellaneous

Get Wind of These Hurricane Tracker Apps | *Cult Of Mac*

Members Helping Members

Need Help? Have a question the manual doesn't answer? Members Helping Members is a group of volunteers who have generously agreed to help. They are just a phone call or an email away. Please call only during the appropriate times, and **only if you are a current mini'app'les member** and own the software in question.

1. Les Anderson	651-735-3953	anderslc@usfamily.net	DEW
2. Tom Ostertag	651-488-9979	tostertag@usfamily.net	DEW
3. Bruce Thompson	763-546-1088	bthompson@macconnect.com	EW
4. Pam Lienke	651-457-6026	plienke@aol.com	DEW
5. Ron Heck	651-774-9151	ronheck@comcast.net	DEW

D = Days, generally 9 a.m. to 5 p.m.
E = Evenings, generally 5 p.m. to 9 p.m.
W= Weekends, generally 1 p.m. to 9 p.m.
NV = No Volunteer

Please call at reasonable hours and ask if it is a convenient time for helping you. By the way, many of these volunteers can also be contacted on our forums. We appreciate your cooperation.

Mini'app'les needs more volunteers for Members Helping Members — If you are willing to be a Members Helping Members volunteer, please send an email message to Membership Director Les Anderson or contact him on our forums with your name, telephone number, contact hours, and the software and hardware areas you are willing to support.

Mini'app'les Membership Application and Renewal Form

Membership cost is $15.00 for one year. To pay electronically using PayPal, visit the mini'app'les website.
If you prefer to pay by check, use the form below. Please make your check payable to "mini'app'les".

Name: _____

Company (if mailed to): _____

Address: _____

City, State, Zip: _____

Phone # (home): _____

Phone # (work): _____

Phone # (cell): _____

Membership ID # (if renewal): _____

Email: _____

Your email address will NOT be sold, shared, or distributed. It will be used only for official mini'app'les business such as distribution of the newsletter and membership renewal reminders.

_____Check if this is a change of address notice

_____Check if you want to volunteer

_____Check if you want to be added to "Members Helping Members"

_____Check if you were referred by a club member (if so, please give member's name)

Please mail this application and your payment to:

mini'app'les
P.O. Box 796
Hopkins, MN 55343-0796

Thank you for your support!

Benefits of mini'app'les Membership

- Access to the mini'app'les online forums. Post questions and/or answers about issues, trouble shooting, products, buying and selling, special events, discounts, and news about Apple and the mini'app'les club.
- Access to our Members Helping Members network of professional and advanced users of Apple technologies. These members volunteer their time to help other members with software, hardware, and other Apple related issues.
- A variety of Mac Special Interest Groups (SIGs) that meet each month.
- Multi-SIG meetings and workshops to help members with computer problems. You can bring your equipment to these events and receive support from knowledgeable Mac users to help diagnose your problem(s).
- Participation in drawings for computer hardware, software, and other computer related materials.
- Discounts from vendors and manufacturers. Refer to the on-line forums for current offers.

mini'app'les

the minnesota apple computer users group, inc.

Introduction — This is the newsletter of mini'app'les, the Minnesota Apple Computer Users' Group Inc., a Minnesota non-profit club. The whole newsletter is copyrighted © by mini'app'les. Articles September be reproduced in other non-profit User Groups' publications except where specifically copyrighted by the author (permission to reproduce these articles must be given by the author). Please include the source when reprinting.

The mini'app'les Newsletter is an independent publication not affiliated, sponsored, or sanctioned by Apple, Inc. or any other computer manufacturer. The opinions, statements, positions, and views are those of the author(s) or newsletter staff and are not intended to represent the opinions, statements, positions, or views of Apple, Inc., or any other computer manufacturer. Instead of placing a trademark symbol at every occurrence of a trade-marked name, we state we are using the names only in an editorial manner, to the benefit of the trademark owner, with no intention of infringement of the trademark.

Questions — Members with technical questions should refer to the Members Helping Members section or bring their questions to an appropriate SIG meeting. Please direct other questions to an appropriate board member.

Dealers — Mini'app'les does not endorse specific dealers. The club promotes distribution of information that September help members identify best buys and service. The club itself does not participate in bulk purchases of media, software, hardware, and publications. Members September organize such activities on behalf of other members.

Submissions — We welcome contributions from our members. Perhaps you're using new software that you just can't live without. Maybe you have a new piece of hardware that you find extremely useful and of high quality. On the other hand, you might be struggling with problematic software or hardware. Why not share your experience with other members by writing a product review? Doing so September steer others towards quality products or help them avoid the problems you September be having.

Submissions must be received by the 15th day of each month to be included in the next month's newsletter. Please send contributions directly to our post office box (mini'app'les, PO Box 796, Hopkins MN 55343), or email them to miniapples@mac.com.

The deadline for material for the next newsletter is the fifteenth of the month. An article will be printed when space permits and, if in the opinion of the Newsletter Editor or Publications Director, it constitutes material suitable for publication.

This newsletter was produced using Apple's Pages word processor.Board of Directors