May 2012

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 major news events this month are: the reported large number of Mac users infected with Flashback malware, Apple's Java Security updates to combat and remove the trojan malware, and the Ebook conspiracy battles. Several applications have announced updates: Audacity, Adobe Flash Player for Mac, and Microsoft Office.

Tom Ostertag, Publications Director

Meeting Calendar

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 – May 2012			
Tuesday	May 1	7:00 pm	Mac OS X SIG
Thursday	May 3	7:00 pm	Mac Applications SIG
Tuesday	May 8	7:00 pm	iOS SIG
Wednesday	May 9	7:00 pm	VectorWorks SIG*
Thursday	May 17	7:00 am	Mac Consultants SIG
Wednesday	May 23	6:30 pm	Mac Q&A SIG
Thursday	May 24	6:30 pm	FileMaker Pro SIG

Meeting Locations and Leaders		
Meeting	**Location**	**Leader**
Mac OS X SIG	Ridgedale Library, 12601 Ridgedale Drive, Minnetonka, MN	Bob Demeules 763-559-1124
Mac Applications SIG	Southdale Library, 7001 York Ave. S., Edina	Tim Drenk, 952-479-0891
iOS SIG	Brookdale Library, 6125 Shingle Creek Parkway Brooklyn Center	Joel Gerdeen, 763-572-0148
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
Mac Q&A SIG	Wentworth Library, 199 East Wentworth Ave E, West St. Paul	Harry Lienke, qasig@miniapples.org
FileMaker Pro SIG	Erik's Bike Shop Corporate, 9201 Penn Ave S. #1, Bloomington	Steve Wilmes, 651-458-1513
* This SIG is NOT sponsored by mini'app'les; the listing is provided as a service to members.		

TABLE OF CONTENTS

mini'app'les Board Meeting • 9 April 2012

by Tim Drenk

Adoption of Agenda - Changes, additions, etc.

- MSP
- Attendance - Tim, Bob, Jeff, Kevin, Les, Bruce (took notes)

Officers and Coordinators Reports

- Treasurer's report: Bob submitted report of current status - MSP
- President's report: Tim will connect Mike with Sandy for database
- Vice President's report: Nothing beyond business
- Secretary's report: Absent
- Publications Director's report: Absent
- SIG Director's report: Kevin doesn't know of any issues with meetings he doesn't attend, like finding locations to meet. There was a question about why the meeting room at Eden Prairie Library closes at 8:30 when the library stays open till 9. Community rooms or schools might be other options to use.
- Membership Director's report: Bert Persson died; Feb renewals sent; 3 pending; Problem with a couple of bounces.
- Past President's report: Sec of State registration

Old Business

- BOD Elections – Tim
  Need counters - Harry Lienke, Les Anderson
- Annual Meeting – Tim, Jeff
  The annual meeting went well; No complaints received
- Website and communication changes – Jeff
  Looking at changing method of email lists - commercial but free mailing lists; possibility of splitting out SIGs.
  When should renewal notice go out? - 2 months; reminder sent after one month; notice of membership lapse; final reminder 30 days later; carry member six months beyond?
  Some method to contact after "bounce".
  Membership cards only upon request
  New member "welcome" email to confirm
  Discussion list to replace Forumer
- Possible SIG Restructuring – Tim
  How can we increase attendance?
  Get ready for September; get ideas together in summer

New Business

- mini'app'les Meeting Possible Dates – Tim
  meeting in Sept - only meeting - Patrick Rhone?
  Another one in March?
  Christmas party in Dec, possibly at the Hack Factory

- BOD meeting reschedule – Tim
  Move to third Monday of every other month.
- Calendar - Set up calendar in new Google account

Adjournment

- Next meeting 7 PM, June 18, 2012 – Southdale Library

---

iOS SIG Meeting • 10 April 2012

by Joel Gerdeen & Tim Tierney

An iOS SIG meeting was held at 7 pm on Tuesday, April 10 at the Brookdale Library. This SIG focuses on iOS devices such as iPhones, iPads, and iPod Touches. Joel Gerdeen was recovering from knee surgery and did not attend so Tim Tierney led the meeting. There was no formal Keynote presentation but just live demos.

We had an interesting and active discussion of favorite apps and techniques, primarily dealing with the iPad. Both Bob Demeules and Sonny had the new iPads and those were briefly discussed with primary focus on the "Retina" screen. Sonny had several hand gestures incorporated into iOS 5 that he demonstrated and used effectively.

The relative features of GoodReader ($5) versus PDF Expert ($10) for organizing and reading documents were discussed. It was believed that PDF Expert had several advantages that made it a good investment. GoodReader remains a reliable choice, however.

Several travel apps dealing with flight itineraries, schedules, and tracks were demonstrated. They included:

Flight Board ($2.99) which keeps track of flight departures and arrivals times and their status.

Flight Track Pro ($9.99) provides live flight status tracking of flights for the traveler.

Trippit (free) is a travel organizer that keeps your plans in one place, according to the App Store. It provides airport information and detailed terminal maps, real-time airplane position, and more.

Live ATC is a free app that allows you to listen in to aircraft related radio traffic, including air traffic control, ground control, etc.

For the frequent traveler these apps provide useful information that could be a real benefit.

Moon Globe HD is a $.99 app by a local developer. It gives a wonderful view of the moon's surface that can be manipulated and zoomed in on. Sites of interest are labeled, including the lunar landing site.

Moonlight Mahjong is another app from this same developer. There is a free version, but the 99¢ paid version offers truly impressive graphics that allow you to manipulate the stack of tiles in 3-dimensions. This was especially stunning on the retina display. It uses the Game Center, or can be played individually. It's worth looking at just for the graphics.

Bob demonstrated Easy QR, a free app that generates QR-Codes for the data you input. This is an app that you can have a lot of fun with.

We then got into discussing and demonstrating different GPS and traffic apps. These included:

MotionX GPS HD and MotionX GPS Drive HD are two similar apps with different applications. They sell for $1.99 and $2.99, respectively, are highly rated, and worth looking into if you're looking for GPS capability for driving, walking, hiking, sailing, flying, etc. Note there are separate iPhone and iPad apps. There may be a fee for continued use after 30 days, but that may not be for all variations of the app (there are four.)

Navigon is a full featured GPS app with a price that reflects it, $50 for the US. (Low ratings and high price justify caution, however.)

Traffic View for iPad is a 99¢ app that shows the locations of traffic cameras on metro maps, indicated as map pins. Click on the map pin of interest and you're presented with the video view from that camera. Very nice if you want to find out where the

delays are, or are not. The Twin Cities are not among the cities listed, but the I-94 area near the river was demonstrated, so it is among those included, but not listed.

Glimpse is a free app for animated viewing of spreadsheet or related data. It appears to be tremendously useful if viewing and interpreting data in a graphic presentation. And it's free.

The next meeting is planned for Tuesday, May 8, at 7:00 PM at the Brookdale Library again, back in Study Room I. The meeting will cover additions to Garageband and continue discussion of favorite apps. For those interested, the meeting will continue afterwards at the nearby Denny's restaurant.

Q&A SIG Minutes • 2 April 2012

by Harry Lienke

The Question and Answer Special Interest Group (Q&A SIG) met, as usual, at the Merriam Park Library. The questions we started with were a continuation of the previous meeting. The member who had updated his iMac's software to Snow Leopard was still having problems. He was unable to get his machine to boot consistently from his install disk or into AppleJack. Initial suggestions were to make sure he updated to OS X 10.6.8 using the Combo Updater to ensure all OS software was at the most up-to-date version and to re-install all of Snow Leopard. Various ways of forcing the iMac to boot from the install disk were mentioned: holding down the Option Key at start-up and picking the install disk from the selections shown, holding down the "C" key at start-up, and setting the System Preferences Startup Disk to select the install disk. To check whether a corrupted start-up application might be causing a problem, one can boot into "Safe Mode" causing the system to boot with only the basic software; non-essential start-up items are not utilized in Safe Mode.

Someone recalled a situation in which inconsistent booting was caused by a wireless keyboard with weak batteries so it was suggested that fresh batteries be used in the iMac's keyboard. Other folks recalled having to wait for their keyboard and computer to synchronize before any data could be entered; this could cause the intermittent boot problems seen but the only suggestion to overcome this was to boot the computer and then restart it after the computer and the keyboard were synced.

A member commented that he had been having problems with his broadband provider slowing down his DSL connection because the provider's equipment was supposedly detecting errors on the line. The member had to instruct the provider several times to set the line at the highest speed because he wasn't detecting any error problems. Someone wondered how to check a modem's speed; he was told the speed can be checked using a browser to access the modem's settings. To check the actual speed of up- and down-loaded data, there are several websites that can be used; these include speedtest.net and speedtest.frontier.com.

A question was asked about programs that could be used to tune up a Mac to get as much speed as possible from it. Programs mentioned include Onyx, Ccleaner, and AppCleaner (with any program of this ilk, you should know what you are doing so you don't disrupt your machine's operation). One member uses AppCleaner to delete specific programs from his machine. It was mentioned that a search tool like EasyFind or FindAnyFile could also be used to seek out and destroy the files associated with a particular application. It was pointed out that some programs like those from Adobe share support files and one must be careful not to delete files used by a program not being deleted. It was noted that yours truly recommends avoiding Adobe Reader (and its many megabytes of support files) and using Preview (a part of the OS X set of tools) to view and change PDFs instead. One can change the default application for viewing PDFs to Preview by doing a Get Info command (Cmd-I) on any PDF document, changing the "Open with" pull-down menu to read "Preview," and then clicking on the "Change All" button located just below that pull-down menu.

Someone wondered what "Adobe Air" is. The answer was it is essentially Flash for the desktop.

Upon machine shut-down, one attendee gets random occurrences of a blue screen with text indicating the system is waiting for a remote debugger. No one at the meeting was familiar with this scenario.

Please note the April Q&A SIG meeting will be held at the usual time (6:30 pm on April 25) at the usual place (Merriam Park Library).

The Merriam Park Library is closed for remodeling during May so the Q&A SIG will meet at the usual time (6:30 pm on May 23) at the Wentworth Library in lovely West Saint Paul. The library is located on Wentworth Avenue a block east of South Robert Street and a few blocks west of US Highway 52. Pie SIG will be held at Bakers Square on South Robert just north of Cub Foods.

How to Detect and Protect Against Updated Flashback Malware

by Adam C. Engst

Apple has released updates to its Java libraries for users of Mac OS X 10.7 Lion and 10.6 Snow Leopard (see "Java for OS X Lion 2012-001 and Java for Mac OS X 10.6 Update 7," 3 April 2012). The updates bring the Java runtime engine up to version 1.6.0_31 and fix multiple vulnerabilities in Java version 1.6.0_29, "the most serious of which may allow an untrusted Java applet to execute arbitrary code outside the Java sandbox." What those release notes aren't saying is that the vulnerabilities in question were being exploited in the wild by a new variant of the Flashback malware (see "Beware the Morphing Flashback Malware," 27 February 2012).

[Update: On 12 April 2012, Apple released updates for Lion and Snow Leopard that removes Flashback, and which are available through Software Update and directly from Apple's support download page. For more information on these updates, see "Apple Releases Flashback Malware Remover," 12 April 2012. Installing the update disables Java on Web pages unless you specifically re-enable Java.]

Significant Infection Rates -- A Russian antivirus developer, Doctor Web, says their research shows more than 550,000 Macs have been infected after users visited compromised Web sites that contain JavaScript code to activate a malicious Java applet. Sorokin Ivan of Doctor Web later raised that estimate to over 600,000 in a tweet. [Update: These had dropped to below 300,000 by April 11.]

Although we haven't seen anything from Doctor Web before, the question of who they are came up on TidBITS Talk, where security analyst Brian McNett said:

> The first I heard of Doctor Web was when they were referenced, and when Sorokin Ivan later responded via Twitter to Mikko Hypponen, Chief Research Officer of F-Secure. I know and trust Mikko. He uses reliable sources. Doctor Web appears to be a Russian outfit, with largely Russian clientele, so it wouldn't be unusual for their reputation to be unknown elsewhere. Their key discovery is that Flashback uses the MAC address of the infected machine as the User-Agent when connecting to its command-and-control server. This is a unique pattern that allowed them to track infections before anyone else. That they shared this finding publicly, along with their data, adds to their credibility.

Mikko Hypponen said in a tweet that F-Secure has spoken with Doctor Web and that the infection numbers look real. And Kaspersky Labs has now provided independent confirmation that Doctor Web's numbers are reasonable and are in fact Macs.

According to Mac security firm Intego, Flashback-infected Macs show no symptoms at all, other than communication with Flashback's command-and-control servers that could be detected by network monitoring tools. Although we haven't seen confirmation of this with recent Flashback variants, earlier versions of Flashback tried to capture user names and passwords by injecting code into Web browsers and other network applications, like Skype. In such cases, the affected programs tended to crash

frequently. Security firm Sophos says that along with stealing passwords, Flashback can also poison search engine results to perform advertising fraud (by fraudulently increasing click-through rate) or to direct victims to further malicious content (though that seems unnecessary, if the Mac is already compromised).

More concerning is that Intego says it has seen dozens of variants of Flashback in the past weeks, indicating that the programmers behind Flashback are modifying it quickly to avoid detection and to take advantage of newfound vulnerabilities. That may render obsolete any advice for preventing, detecting, and removing Flashback. On a side note, Intego also says that it has evidence that Flashback was created by the same people who created MacDefender in 2011 (see "Beware Fake MACDefender Antivirus Software ," 2 May 2011 and "Apple Responds to Increasingly Serious MacDefender Situation," 25 May 2011).

Detect Flashback Infection -- So how can you tell if you're infected? Security firm F-Secure posted instructions for detecting current Flashback infections; the instructions also include removal steps that we would dissuade anyone but advanced users from attempting.

That said, detection comes down to issuing the following defaults read commands in Terminal (F-Secure suggests only the first and last; the others extend the technique from Safari to Google Chrome, Firefox, and iCab). In each case, if you see "does not exist" at the end of the response from each command, you are not infected. (The defaults read command is entirely safe — it's just attempting to determine whether some data exists in the Info.plist file within each application package.)

```
defaults read /Applications/Safari.app/Contents/Info LSEnvironment

defaults read /Applications/Google\ Chrome.app/Contents/Info LSEnvironment

defaults read /Applications/Firefox.app/Contents/Info LSEnvironment

defaults read /Applications/iCab\ 4/iCab.app/Contents/Info LSEnvironment

defaults read ~/.MacOSX/environment DYLD_INSERT_LIBRARIES
```

For a simpler approach, Marc Zeedar, publisher of Real Studio Developer magazine, has written a simple Test4Flashback application that encapsulates the defaults read checks and presents a dialog telling you whether or not you're infected. It doesn't attempt to do any removal at all.

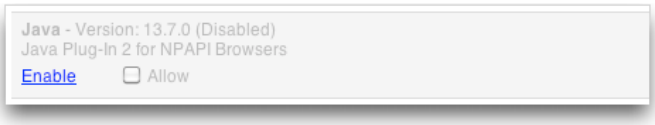
Protect Yourself Against Flashback -- In the meantime, if you are using 10.7 Lion and have not yet installed Java, hold off unless you need it. If you have installed Java in Lion or are using 10.6 Snow Leopard, immediately install Apple's Java updates via Software Update to prevent infection from this particular variant of Flashback. And although uninstalling Java is difficult, you can disable it, either system-wide or in individual Web browsers (Flashback relies entirely on Web-based attacks, as far as we're aware).

To disable Java entirely on your Mac, open the Java Preferences utility in /Applications/Utilities and uncheck the checkboxes. Don't do this if you use CrashPlan or any other Java-based software, including some Adobe applications!

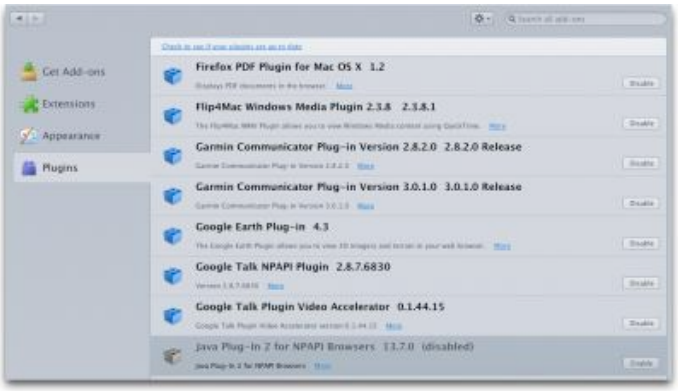
• To disable Java in Safari, choose Safari > Preferences, and turn off Java in the Security pane.

• To turn off Java in Google Chrome, type about:plugins in the address bar, scroll down, and click the Disable link for Java Plug-In 2 for NPAPI Browsers.

• To turn off Java in Firefox, choose Tools > Add-ons, click the Plugins tab, and disable the Java Plug-In 2 for NPAPI Browsers.



If you need to use Java only occasionally, consider leaving it enabled in a browser that you seldom use, and rely on that browser for those specific sites — like Web conferencing tools — that require Java.



Installing antivirus software like Intego's VirusBarrier will also provide protection, both from the software's base functionality and because the Flashback malware doesn't install itself if it detects certain antivirus programs.

Lastly, it's worth noting that some variants of Flashback worm their way onto Macs not through exploiting Java vulnerabilities, but by fooling users into entering an administrator password. The only way you can protect yourself against such trickery is by being suspicious of any password request that doesn't come in direct response to an action that you've just taken, such as installing a new piece of software that you downloaded intentionally.

Be careful out there.

How to Tell If Your Cloud Provider Can Read Your Data

by Rich Mogull

With the tremendous popularity of services like Dropbox and iCloud there is, rightfully, an incredible amount of interest in cloud data security. Once we start hosting our most sensitive data with cloud services (or any third-party provider) it's only natural to wonder how secure our data is when it's in the hands of others. But sometimes it's hard to figure out exactly *who* can look at our information, especially since buzzwords like "secure" and "encrypted" don't necessarily mean *you* are the only one who can see your data.

How Cloud Providers Protect Your Data -- In part because there are numerous ways cloud providers could protect your data, the actual implementation varies from service to service. All consumer cloud services are what we in the cloud world call *public* and are built for *multi-tenancy*.

A public cloud service is one that anyone on the Internet can access and use. To support this the cloud providers need to *segregate* and *isolate* customers from each other. Segregation means your data is stored in your own little virtual area of the service, and isolation means that the services use security techniques to keep people from seeing each other's stuff.

Practically speaking, multi-tenancy means your data is co-mingled with everyone else's on the back end. For example, with a calendar service your events exist in the same database as all the other users' events, and the calendar's code makes sure your appointment never pops up on someone else's screen. File storage services do the same thing: intermingling everyone's files and then keeping track of who owns what in the service's database. Some, like Dropbox, will even store only a single version of a given file and merely point at it from

different owners. Thus multiple users who happen to have the same file are technically sharing that single instance; this approach also helps reduce the storage needed for multiple versions of a file for a single user.

Although multi-tenancy means co-mingling data, the cloud provider uses segregation techniques so you see only your own data when you use the service, and isolation to make sure you can't maliciously go after someone else's data when you're using the system.

The cloud provider's databases and application code are key to keeping all these bits separate from each other. It isn't like having a single hard drive, or even a single database, dedicated to your information. That simply isn't efficient or cost-effective enough for these services to keep running. So multi-tenancy is used for files, email, calendar entries, photos, and every other kind of data you store with a cloud service.

Not all services work this way, but the vast majority do.

Encryption to the Rescue? -- A multi-tenancy architecture has two obvious problems. The first is that if there's a mistake in the application or database the service runs on, someone else might see your data. We've seen this happen accidentally; for example, last year Dropbox accidentally allowed any user access to any other user's account. There is a long history of Internet sites (cloud and otherwise) inadvertently allowing someone to manipulate a Web page or URL to access unauthorized data, and the bad guys are always on the lookout for such vulnerabilities.

The second problem, which has been in the press a lot lately, is that the cloud provider's employees can also see your data. Yes, the better services usually put a lot of policy and security controls in place to prevent this, but it's always technically possible.

One way to mitigate some of these concerns is with encryption, which uses a mathematical process coupled with a digital key (a long string of text) to turn your data into what looks like random gibberish. That key is necessary to decrypt and read the data.

Most cloud providers use encryption to protect your Internet connection to them (via SSL/TLS — look for https URLs) so no one can sniff it on the network. (Unfortunately, some large email providers still don't always encrypt your connection.) Most of the time when you see "encryption" in a list of security features, this is what they mean. But encrypting data in transit is only half the battle — what about your data in the provider's data center? Encryption of storage is also necessary for any hope of keeping your data secret from the cloud provider's employees.

Some providers do encrypt your data in their data center. There are three ways to do this:

1. Encrypt all the data for all users using a single key (or set of keys) that the cloud provider knows and manages.
2. Encrypt each individual user's data with a per-user key that the *cloud provider* manages.
3. Encrypt each individual user's data with a per-user key that the *user* manages.

By far, most cloud services (if they encrypt at all) use Option #1 — keys that they manage and that are shared among users — because it's the easiest to set up and manage. The bad news is that it doesn't provide much security. The cloud provider can still read all your data, and if an attacker compromises the service's Web application, he can usually also read the data (since it's decrypted before it hits the Web server).

Why do this level of encryption at all? It's mostly to protect data if a hard drive is lost or stolen. This isn't the biggest concern in the world, since cloud providers have vast numbers of drives, and it would be nearly impossible to target a particular user's data, if the data could be read at all without special software. It also means that providers get to say they "encrypt your data" in their marketing. This is how Dropbox encrypts your data.

Option #2 is a bit more secure. Encrypting every user's data with an individual key reduces, in some

cases, the chance that one user (or an attacker) can get to another's data. It all depends on where the attacker breaks into the system, and still relies on good programming to make sure the application doesn't connect the wrong keys to the wrong user. It's hard to know how many services use this approach, but when done properly it can be quite effective. The major weakness is that the cloud provider's employees can still read your data, since they have access to the keys.

Option #3 provides the best security. You, the user, are the only one with the keys to your data. Your cloud provider can never peek into your information. The problem? This breaks... nearly everything. First of all it means you are responsible for managing the keys, and if you lose them you lose access to your data. Forever. Also, it is extremely difficult — if not impossible — to allow you to see or work with your data in a Web page since the Web server can't read your data either. Thus it works for some kinds of services (mostly file storage/sharing) and not others, and *only* for sophisticated users who are able to manage their own keys.

As is so often the case, these options reveal the tradeoff between security and convenience.

How to Tell if Your Cloud Provider Can Read Your Data -- In two of the three options I listed above, the provider can read your data, but how can you tell for yourself if this is the case?

There are three different (but similar) indications that your cloud data is accessible to your provider:

- If you can see your data in a Web browser after entering only your account password, the odds are extremely high that your provider can read it as well. The only way you could see your data in a Web browser and still have it be hidden from your provider is if the service relied on complex JavaScript code or a Flash/Java/ActiveX control to decrypt and display the data locally.
- If the service offers both Web access and a desktop application, and you can access your data in both with the same account password, odds are high that your provider can read your data. This is because your account password is also probably being used to protect your data (usually your password is used to unlock your encryption key). While your provider could technically architect things so the same password is used in different ways to both encrypt data and allow Web access, that really isn't done.
- If you can access the cloud service via a new device or application using your account user name and password, your provider can probably read your data. This is just another variation of the item above.

This is how I knew Dropbox could read my files long before that story hit the press. Once I saw I could log in and see my files, or view them on my iPad without using a password other than my account password, I knew that my data is encrypted with a key that Dropbox manages. The same goes for the enterprise-focused file sharing service Box (even though it's hard to tell when reading their site). Of course, since Dropbox stores just files, you can apply your own encryption before Dropbox ever sees your data, as I explained last year at Securosis.

And iCloud? With iCloud I have a single user name and password. It offers a rich and well-designed Web interface where I can manage individual email messages, calendar entries, and more. I can register new devices and computers with the same user name and password I use on the Web site. Thus, from the beginning, it was clear Apple had the capability to read my content, just as Ars Technica reported recently.

That doesn't mean Dropbox, iCloud, and similar services are insecure. They generally have extensive controls — both technical and policy restrictions — to keep employees from snooping. But it does mean that such services aren't suitable for all users in all cases, especially businesses or governmental organizations that are contractually or legally obligated to keep certain data private.

Doing It Right -- The backup service CrashPlan is an example of a service that offers flexible encryption to fit different user needs, with three separate options. (For more on choosing the

appropriate encryption method for CrashPlan, see Joe Kissell's "Take Control of CrashPlan Backups.")

First, by default, your data is encrypted using a key protected by your account password. This still isolates and protects it from other users, while enabling you to view file information through the CrashPlan Web site and the CrashPlan Mobile app. But CrashPlan's employees could still access your data.

Second, if you want more security, you can add a separate backup password that only you know. This approach still allows access through the CrashPlan Web site and the CrashPlan Mobile app, but CrashPlan employees can't see your data except (maybe) during a Web session after you enter your separate password. Attackers can't access your data either, though your password may be susceptible to brute force cracking or social engineering.

Third and finally, you can generate your own per-device encryption keys, which CrashPlan never sees or knows about, rendering your backups readable only by you (or anyone who can beat the key out of you — never underestimate the power of a wrench — props to xkcd!). You could technically use a different encryption key on each device (or share, your choice) so that even if one system were to be compromised, it wouldn't allow access to backups from your other devices. Clearly, this is much more difficult to manage and well beyond the needs or capabilities of the average user (heck, even I don't use it).

So if you want to be certain that your data is safe from both attackers and the cloud provider's employees snooping, look for services that offer additional options for encrypting data, either with a password or an encryption key known only to you. If such an option isn't available at the next cloud service you check out, you'll know that the provider's employees could technically read your data. And when the next big story of a cloud provider reading data hits the headlines, you can smugly inform your friends that you knew it all along.

Notes, Quotes, and iBooks

by Michael E. Cohen

Anyone who knows me knows I have a book problem: I have books on the shelves, books in boxes, books on my nightstand, books on my tables, books on the floor, books in a locker, books on the backseat and in the trunk of my car. My books take up an amazing amount of room, and, while I wouldn't want to part with them, they can be inconvenient, especially when I need space in my home for something else (like, say, stacks of magazines and journals). My plenitude of books can also be inconvenient when I want to look something up in a volume that needs to be disinterred from deep within one of my various book stashes.

That's why I welcomed the onset of the era of ebooks a few years ago. With ebooks, the physical volume problem evanesces: I can now carry more books in my pocket than I can stack on my dining room table and have each readily available with a few taps and swipes. For someone like me, whose bibliophilia occasionally approaches mild bibliomania, ebooks are a gift from heaven.

Of course, ebooks are not without their inherent drawbacks: they require expensive readers, they stop working when the battery goes dead, they just don't look as nice (even with a Retina display) as a well-designed printed book, and so on. I can accept *inherent* drawbacks.

What I find unacceptable are arbitrary drawbacks that are created *deliberately* by those who design and develop ebook-reading software. In particular, I'm appalled by the shortcomings with notes and quotes that ebook software developers design into their products, especially in light of the growing movement to replace traditional textbooks with their ebook equivalents.

Here are two things that students (and, in fact, many active readers) do with books:

- They mark them up with notes and highlights.
- They quote from them.

The designers of ebook reading software have hobbled, by choice, these readerly activities. Let's take a look at how one ebook-reading app, Apple's iBooks, tosses obstacles in the student's path. Lest you think I'm picking on iBooks, keep in mind that most other ebook-reading apps exhibit similar shortcomings.

Notes -- At first glance, iBooks provides a breakthrough in book-marking power for the active reader. You can highlight passages in a variety of colors with just a swipe of the finger, and attach notes of arbitrary size to any passage without worrying whether there's enough space in the margin to encompass your thoughts. Even better, you can take a quick trip to the Table of Contents in iBooks to see all of your notes and markups, along with their context, and get to any of them with a single tap. Sweet.

Not sweet? Getting those notes and markups out of the book so you can use them elsewhere. Tap the Share button (that swooshy arrow in a box) on the upper-right corner of the Notes page and you see the tantalizing options to print your notes and send them via email. And it's true: you can do these things. What you can't print or email is the *context* attached to each note. The passage that you highlighted, and which appears on the Notes page in iBooks, is not included in whatever is printed or sent via email. All you get is your note and an almost useless chapter name (or, in the case of a textbook, a page number) to accompany it. If margin notes constitute a conversation between a book and its reader, the exported notes in iBooks give you only one side of that conversation.


Subject: Notes from "What's Next for Text", Chapter 12: Large Scale Alternations

NOTES FROM

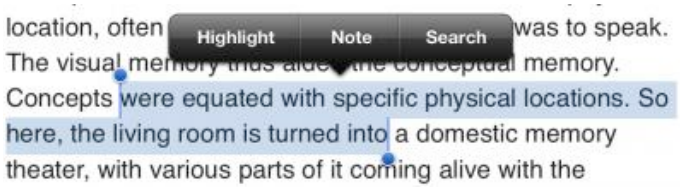
What's Next for Text

Large Scale Alternations, p. 42 April 4, 2012

Important concept

Quotes -- Students quote from books all the time. In fact, it is an activity that is often required by specific instructional assignments. Learning how to quote properly, cite accurately, and integrate quotations effectively into an argument are fundamental writing skills that students must learn. Yet iBooks provides scant help for this basic activity.

Certainly, if one is reading an unprotected ebook in iBooks, any selected text in the book is available for copying to the clipboard, from where it can be pasted into a word processing document, email message, or other text container. But that works only for unprotected books, and only for those ebooks in EPUB format. Surprisingly, even in an unprotected textbook produced by iBooks Author (which use Apple's own proprietary Multi-Touch book format) the Copy command for selected text is missing in action.



For protected EPUBs, it seems that a design decision was made to disable copying, most likely in an attempt to deter piracy. No matter that a pirate would have to copy each page of a book separately (you can't select across page boundaries in iBooks), and no matter that a pirate could just as easily (which is to say, not very) take screen captures of each page and use OCR software to make a pirated version.

But disabling copying from even an unprotected textbook? What is the point of that? A fear, perhaps, that students might plagiarize from a textbook that their teachers have assigned? Possibly, but it would be a very dim student indeed who would plagiarize content from a book that a teacher would almost certainly be able to recognize. If that's the reason, it is a silly one.

We've Solved These Problems Before -- As far as I can tell, these design limitations regarding notes and quotes are imposed merely to deter "theft" (so quoted because the activities that these software

limitations attempt to deter are not theft but instead infringement and plagiarism).

The old Voyager Expanded Books, the floppy-disk-based ebooks produced back at the dawn of ebooks in the early 1990s, solved the infringement/plagiarism problem another way: not by restricting the use of a book's contents, but by encouraging correct use. Exported notes from Expanded Books included the text to which they were attached, along with a complete citation. Text copied to the clipboard also included a citation appended to the text.

The Expanded Book designers (of whom I was one) realized that deliberate piracy is nearly impossible to stop. We also knew that throwing obstacles in the paths of honest readers to deter piracy was a poor strategy for stopping it: it would make honest readers snarl, while the pirates would only laugh.

And what about plagiarism? For deliberate, determined plagiarists, we applied the same reasoning we used for pirates. As for unintentional plagiarists (and a large number of student plagiarists fall into that category), we felt that the addition of a citation to each copied passage served as model and a lesson for students: quoted text should always include an attribution. We made a possible problem into an opportunity for instruction.

It would not be difficult for iBooks, and other ebook-reading apps, to incorporate similar behaviors for copied and annotated text. It would be harder, I suspect, to convince publishers that books are not merely containers of words that the reader passively consumes, but containers of thoughts, ideas, and opinions with which the reader actively interacts. But publishers need to come to that realization if ebooks are to become fully capable substitutes for the bound volumes that have colonized my home and are pushing me out into the street.

Until they do, though, ebooks will remain intentionally flawed crippleware, which is a real shame.

You can quote me on that.

Use Dropbox to Troubleshoot Family Macs

by Jeff Carlson

The Flashback malware that reportedly infected more than half a million Macs creates the kind of situation that's ripe for confusion by friends and family members who aren't technologically savvy. (See "How to Detect and Protect Against Updated Flashback Malware," 5 April 2012.) When news bubbles up to the mainstream media, those of us who help manage these remote Macs often get calls or emails asking for help.

Apple this week released an update to Java that removes the malware, so anyone that runs Software Update can protect themselves against the threat (see "Apple Releases Flashback Malware Remover," 12 April 2012). But before that update, I wanted to check my family members' Macs for infection, something made much easier thanks to Dropbox. Whether you need to quickly share family photos or troubleshooting utilities, the process I describe here makes it easy to distribute files among many Macs, even if they're not all owned by you.

I wanted to send Marc Zeedar's Test4Flashback application, which could tell immediately whether Flashback has infected a system, to the iMacs owned by my mother and mother-in-law. I'd previously set up Dropbox on both of their systems, and created a "Jeff" folder on each. Getting the app to their machines was a simple matter of copying it to each folder. Dropbox then synchronized the file to their computers (and since I did this in the middle of the night, I wasn't disrupting either of them — and the program is tiny).

The next day, I called my mother and asked her to run the app; her iMac was not infected. For my mother-in-law's iMac, I connected remotely using a LogMeIn account I'd previously set up and ran the app myself; hers was also Flashback free.

Dropbox is ideal for transferring files like this to family members, and better than sending email attachments — which could get caught in email filters — or attempting file transfers via iChat. And since Dropbox offers 2 GB of free storage space, it doesn't cost a thing. In fact, with last week's news that Dropbox was increasing the amount of storage it gives for referrals, you and your friend can both benefit (see "Dropbox Referral Bonuses Doubled to 500 MB, Retroactively," 4 April 2012).

Hot Links:
Compiled by Tom Ostertag

Apple, Inc.

Get Digital Copies Of Your Mac Manuals | *MacWorld*

Apple Rolls Out New Security Measures For iTunes, App Store | *AppleInsider*

Mac Software

New Trojan Variant Can Install Without Password | *MacWorld*

New FileMaker 12 Software Line Released Today | *Apple Hot News*

Apple Java Update Removes Flashback Malware | *AppleInsider*

'Flashback' Trojan Estimated To Have Infected 600K Macs Worldwide | *AppleInsider*

Kapersky Lab Offers Free Scanning And Cleanup For Flashback Malware | *Edible Apple*

Apple Updates Java For A Third Time, This Time With Flashback Malware Removal | *Infinite Loop*

Apple To Release Flashback Removal Software, Working To Take Down Botnet | *Infinite Loop*

Microsoft Office For Mac 2011 14.2.0 | *TidBITS*

IPhoto '11 9.2.3 | *TidBITS*

Adobe Releases First Flash Player 11.3 Beta For Mac OS X | *Cult Of Mac*

Mac Hardware

Thunderbolt storage roundup: The hair-pulling irony | *CNET*

iPad/iPod/iPhone/iTunes/iOS

Instant Expert: Secrets & Features of iTunes 10.6 | *iLounge*

This Ideas App Has A New Idea For Managing Your Ideas [Review] | *Cult of Mac*

Customize Spotlight to Search Smarter [iOS Tips] | *Cult of Mac*

Free on iTunes: 3 Free iPad Apps For Going Places | *The Mac Observer*

iTunes 11 rumored to include under-the-hood changes, iCloud support | *Infinite Loop*

Adding Attachments to iCloud Calendar Events | *iLounge*

Understanding iTunes Authorizations | *MacNews*

Miscellaneous

Seven Ways To Free Up Drive Space | *MacWorld*

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@q.com	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 may 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 may help members identify best buys and service. The club itself does not participate in bulk purchases of media, software, hardware, and publications. Members may 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 may steer others towards quality products or help them avoid the problems you may 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

President	Tim Drenk 952-479-0891 timdrenk@miniapples.org
Vice President	Jeff Berg 781-350-0598 jeff@purpleshark.com
Secretary	Joel Gerdeen 763-607-0906 jgerdeen@mac.com
Treasurer	Bob Demeules 763-559-1124 osx.sig@mac.com
Membership Director	Les Anderson 651-735-3953 anderslc@usfamily.net
Publications Director	Tom Ostertag 651-488-9979 tostertag@q.com
SIG Director	Kevin Strysik 65l-489-4691 strysik@mac.com
Director at Large	Bruce Thompson 763-546-1088 bthompson@macconnect.com
Membership Coordinator	Sandy Foderick sfoderick@mac.com