May 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:
We have two articles in this newsletter written by Jeff Berg, one on Mac Security and the other on the accusation that Apple is watching you. Both are interesting. I have also been doing some research on a new iMac to replace my ancient 1997 Beige G3. Interestingly, a fully loaded 27" iMac costs less than my first Apple //e and that was purchased in 1983.

I've had an interesting month reading all the news feeds and watching the new developments in Lion, Mac OS X 10.7, and Thunderbolt.

Tom Ostertag, Publications Director

Meeting Calendar
At the right is a list of mini'app'les meetings for May 2011. The 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 2011			
Tuesday	May 3	7:00 pm	Mac OS X SIG
Thursday	May 5	7:00 pm	Mac Applications SIG
Tuesday	May 10	7:00 pm	iOS SIG
Wednesday	May 11	7:00 pm	VectorWorks SIG*
Thursday	May 19	7:00 am	Macintosh Consultants SIG
Monday	May 23	6:30 pm	Mac Q&A SIG
Thursday	May 26	6:30 pm	FileMaker Pro SIG

Meeting Locations and Leaders		
Meeting	**Location**	**Leader**
FileMaker Pro SIG	Erik's Bike Shop Corporate, 9201 Penn Ave S. #1, Bloomington	Steve Wilmes, 651-458-1513
Mac Applications SIG	Wescott (Eagan) Library, 1340 Wescott Road, Eagan	Tim Drenk, 952-479-0891
Mac OS X SIG	The Foundation, 311 7th Ave North, Minneapolis	Bob Demeules, 763-559-1124
Macintosh Consultants SIG	Good Day Café, 5410 Wayzata Blvd., Golden Valley	Bob Demeules, 763-559-1124
iOS SIG	Southdale Library, 7001 York Avenue South, Edina	Joel Gerdeen, 763-607-0906
VectorWorks SIG*	CJR Office, 4441 Claremore Dr., Edina	Charles Radloff, 952-941-1667
Mac Q&A SIG	Merriam Park Library, 1831 Marshall Ave., St. Paul	Chuck Hauge, 612-963-5064
* This SIG is NOT sponsored by mini'app'les; the listing is provided as a service to members.		

TABLE OF CONTENTS

BOD Meeting Minutes • April 11, 2011

Submitted by Joel Gerdeen

In attendance: Tim Drenk, Joel Gerdeen, Bruce Thompson, Dave Lundin, Kevin Strysik, Les Anderson.

Absent: Tom Ostertag, Dave Diamont

Other Attendees: None

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

Minutes: The minutes for the December 13, 2010, BOD meeting were approved electronically and published on forumer.com by Bruce Thompson on December 27.

Directors' Reports

Treasurer Dave Lundin's report: All bills are paid. A written report was presented. Dave will research our liability insurance which hopefully will result cost savings.

President Tim Drenk report: See below.

Vice President Dave Diamont report: Dave has moved back to California and will no longer participate.

Secretary Joel Gerdeen's report: Published last report on Nov 22 and missed a portion of the Dec meeting before connecting remotely. The December report was written by Bruce and Tim reported on the Annual meeting in Feb.

Publications Director Tom Ostertag's report: No report.

SIG Director Kevin Strysik's report: Problem with Foundation opening doors for OSX SIG. May need to confirm our contact and meeting schedules. Minor conflict with Twins games as well.

Membership Director Les Anderson's report: Twenty-one members renewed over the last two months. Problem with a member's card showing date of joining back in 1981 was being investigated.

Past President Bruce Thompson's report: Continued with free MobilMe account which is used for group calendar. iDisk for membership data.

Old Business

iOS SIG - Joel volunteered to lead the iOS SIG was first held on January 11 with further meetings in Feb, March and April. Turnout has been average with 7 to 10 members as each meeting. Separate reports are published in the newsletter.

New Business

Need new webmaster - Looking for a volunteer to manage the web site hosted on bluehost.

SWOT Review - Reviewed the SWOT analysis conducted in the Fall of 2009. SWOT is a strategic planning method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats. SWOT recommendations were reviewed and evaluated as how best to implement them. Decided to add discounts that the group received to the newsletter if timely.

Mac Main Meeting - We decided to plan a joint meeting of the main SIGs (OSX, iOS, Mac Apps & Q&A) for Thursday, Sept 15. During Sept, these SIGs will not meet separately though the Filemaker and VectorWorks SIGs will meet as normal. The location remains to be determined and additional promotion will be used to get the members out and recruit new members.

Tim Tierney's Proposal - Tim T. had submitted a proposal to the BOD to amend the SIG Leader guidelines of April 2007. He proposed restricting SIGs from presenting applications costing over $100 or related to controversial subjects such as religion or politics. The BOD rejected this proposal but recommends that all SIG leaders notify attendees in advance about the meeting subject and agenda.

In Addition - Ballot counters were designed to count the ballots of the election and the food bill from the annual meeting was approved.

Next meeting: Scheduled for June 13, 2011 at the Southdale Library at 7:00 pm. All club members are welcome to attend.

The meeting ended at 8:45pm

iOS SIG Meeting • 12 April 2011

by Joel Gerdeen

The fourth iOS SIG meeting was held on Tuesday, April 12, at the Southdale branch of the Hennepin County Library. This SIG focuses on iOS devices such as iPhones, iPads, and iPod Touches. Joel Gerdeen led the meeting and presented the new iPad 2 and related new apps released with iOS 4.3 There was good discussion and feedback from the 4 mini'app'les members that attended.

This meeting was conducted without any video camera or intermediate connection to a projector. The iPad 2 was connected through the VGA adapter to the room projector mounted in the ceiling which displayed the iPad on a large screen in front of the room. A portion of the meeting was presented through Keynote on the iPad but most of the meeting was a demonstration of apps on the iPad. The new mirroring capability of the iPad 2 showed the full iPad screen on the large projection screen. The new iPhone Hotspot capability was demonstrated to connect the iPad through the iPhone to the internet. Facetime, Photobooth, iMovie, Garageband, iAD Gallery, the Mercury web browser, and the Bento update were also demonstrated. The Keynote viewgraphs, available on the iWork.com site, include links to the demoed apps. After the meeting, the attendees met at the nearby Bakers Square for further discussion.

The next meeting is planned for Tuesday, May 10th at 7 PM at the Southdale Library Public Conference meeting room. The subject of the meeting will cover more details of the new iMovie and GarageBand apps.

MacApps SIG Meeting Minutes • 7 April 2011

By Tim Drenk

For the April Mac Apps SIG, Jon Parshall of CodeWeavers (http://www.codeweavers.com) presented CrossOver Impersonator. CrossOver allows Mac users (or Linux users) to install and run Windows programs without running Windows OS.

CrossOver uses a compatibility layer called Wine to do this so it is not an emulator like Parallels or Fusion. An advantage of CrossOver instead of using an emulator is it can be faster, both starting and running the application. Instead of having to start and wait for Windows to load, CrossOver loads the application directly. Plus the overhead of a second OS is not there. Another advantage is the viruses, trojans, and other Windows malware are not a threat; since the full Windows OS is not loaded, the malware is unable to exploit Windows' weaknesses.

The main disadvantage of using CrossOver is that not all applications are compatible with it. CodeWeavers maintains a compatibility database (http://www.codeweavers.com/compatibility/) of programs that are known to work or not work with CrossOver. If the program that someone wants to use with CrossOver is not listed in the database, Jon suggested downloading the free demo and trying the application with it.

CodeWeavers provides a CrossTie installation process for over 900 programs. A CrossTie installer essentially automates the install process for the program. To install Office 2007 for Windows, I can download the CrossTie installer, insert my install CD, and let the CrossTie installer run. It takes care of the installation and when it's finished, I am able to run Office 2007. If there is not a CrossTie installer for a program, CrossOver can step through the install process manually.

There are two different versions of CrossOver, Standard and Pro. The difference is primarily the length of support and updates available. The Standard version ($40) comes with six months of support and updates. The Pro version ($70) comes with twelve months of support and updates and can be renewed for $35. Keep in mind, even if support ends, CrossOver will continue to work. Updates are only critical if you are trying to run a recent program or an unsupported program that becomes supported. But if you install and run a program and it works, no support or updates are necessary.

Jon gave away two full versions of CrossOver Pro. I want to thank Jon for his time and willingness to share with us.

The May meeting will be on Thursday, May 5th, at the Eagan Wescott Library at 7:00 pm. We will be looking at DEVONthink and Evernote, two applications designed to store and organize your information and files.

Mac OS X SIG • April Meeting Report

by Jeff Berg

Bob DeMeules was off on vacation so I had the privilege of presenting and moderating the discussion at the April meeting. Attendance was light, which I hope was due to the Spring-like weather and not a reflection on the moderator. Those in attendance arrived to a dark, locked building. A phone call and some social engineering fixed this. Many thanks to the support tech at Atom who fielded my call, checked our bonafides, and ultimately let us into the building.

While setting up the projector, we had our regular discussion of Apple and tech news. After that, following up on a topic from a prior meeting, we took a quick look at Namebench, a free utility for benchmarking and choosing the best Domain Name System servers for your network. The right DNS server can significantly increase "internet speed".

This speed increase is particularly noticeable when downloading large files or streaming video from services like Netflix. Namebench makes it easy to compare the performance of different DNS servers on your network and recommends the best choices based on common criteria or, should you choose, your own web-surfing habits.

Our main topic was security. We covered some basic security concepts, discussed Apple's approach to security, and looked at some of the core technologies that make OS X and iOS secure. We concluded with practical tips for securing our Macs. (See Security: Mac OS, iOS and You elsewhere in this issue.)

The meeting adjourned approximately 15 minutes later than scheduled and quickly devolved, as all meetings do, into further discussion and a pie-eating frenzy at our secret offsite location, Codename: Perkins.

Q&A SIG Meeting • 28 March 2011

By Les Anderson

A large number of topics were covered at the March 28 Q&A SIG meeting led by Les Anderson. Chuck Hauge had a conflict and couldn't be at the meeting. We started off with a demo of CoconutBattery. It measures the battery life cycle in your MacBook or MB Pro. See article in last month's Newsletter. There was also a demo of Aviary which allows a user to print or save an entire web page without doing "Screen Shots".

The discussion turned to various utilities and some of the pros and cons. Cleaning programs often cause more problems because they can delete necessary files. Other utilities mentioned were ONYX, TechTool Pro, Namebench, and Crossover, the subject of the MacApps SIG held the following week. Macupdate.com is having a bundle sale and about a dozen utilities can be purchased at a very good discount. It included TechTool Pro and 1PASSWORD. KimKamando.com also has a tested list of Shareware/Freeware programs <http://www.komando.com/downloads/> for both Mac and PC.

Several members offered tip or suggestions. Never buy on-line in a public place even with your own computer. One member had his e-mail hacked while in a cafe and using his computer. It was also reported that there may be problems with OSX 10.6.7. Also discussed was the new Safari and iChat in OS X 10.6. Another suggestion was to set up an emergency e-mail if you are using gMail.

We also discussed Remote Access programs such as TeamViewer and the capability of iChat to allow remote access as well.

Security: Mac OS, iOS and You

by Jeff Berg

A presentation to the mini'app'les Mac OS X SIG, 5 April 2011

Mac Users put faith in the belief that our computers are more secure than Windows machines. Critics say this is false sense of security. They attribute the lack of threats to the platform's minority market share. The truth is somewhere in the middle. It's true, Macintosh offers a smaller number of targets and benefits somewhat from the relative obscurity, but there are also specific features that Apple built in to Mac OS (and iOS) to protect our devices from break in, data theft, and malware. Most users can rest easy, knowing that Apple has their back.

SecurityThink

"Security is a process, not a snapshot". [Shawn Geddis, Enterprise Security Consulting Engineer, Apple Inc.] You can't read an article online, blindly follow instructions to install special software or set a few preferences, and consider yourself to be "safe". Everyone's needs are different. We all face different threat levels and have varying tolerance of risk. As Geddis puts it, "There are no silver bullets".

According to Security guru Bruce Schneier effective security requires compromise. [Balancing Security

and Usability in Authentication] Security comes at the expense of freedom and usability. The goal of a 100% percent secure system is a fallacy. The system would be unwieldy, impractical to use. Even if it were desirable, total security is improbable. "Security is a continuum and 100% elimination of a Vulnerability is rarely possible." [Roger G. Johnston. Being Vulnerable to the Threat of Confusing Threats with Vulnerabilities] Everyone has a unique, personal sweet spot on this continuum where security and freedom are balanced.

Unfortunately, we tend to make poor decisions when it comes to security. "Security is both a feeling and a reality. And they're not the same." This leads to poor risk assessment and a misappropriation of security resources. [Bruce Schneier, The Psychology of Security] Your decisions are also influenced by your perception of security models. [Rick Wash. Folk Models of Home Computer Security] You might think you're an unworthy target for computer criminals and take minimal security precautions — not recognizing the value of your computer and internet connection as part of a botnet. At the other extreme, overestimating your risk, or paying too much attention to Movie Plot threats [Schneier], may cause you to lock systems down too tightly. This negatively impacts usability and wastes resources.

Finally, it's important to recognize the difference between a vulnerability and a threat. We are vulnerable to bullets. A loaded gun pointed in your direction is a threat. Most of the security "warnings" for the Mac OS reference vulnerabilities. They don't become threats until someone exploits them. That being said, we are better off understanding and addressing vulnerabilities because threats can come from many directions and a single vulnerability can be exploited by multiple threats. [Johnson]. Most computer virus protection addresses specific threats and does nothing to address the underlying vulnerabilities.

Apple's Approach

Mac OS and iOS are developed with a secure foundation. Security is not an afterthought, it is Built-in, Not Bolted-on. Apple presumes the user won't be a computer guru, so security needs to be Industrial Strength, User-Friendly. Understanding that when faced with a choice about security, most users will make the wrong decision [Geddis but Schneier also makes this point regularly], Apple seeks to provide Protection without Administration. Recognizing that most computers are administered by non-experts, and that threat vectors are numerous and constantly changing, Apple focuses on defending against things you don't know that you don't know. [Geddis] I like to think of this as Apple's own version of Defense against the Dark Arts. You may not know what's attacking you, but there are powerful forces protecting you. [The phrases shown in bold in this paragraph are from Apple presentation slides.]

Security in Mac OS X

Mac OS X provides a layered defense that protects data at all levels: Internet, Applications, Network, OS, and Hardware. Protections include malware protection, strong cryptography, user files encryption, strong authentication, application level firewall, secure network connections, application signing, sand-boxing, library randomization and initial quarantine of downloaded applications. Most of OS X security is standards based and has roots in the open source community. This allows those so inclined to beat on it in search of vulnerabilities.

Good security requires Strong Authentication. Authentication, or "proof of who you are", is generally established by something you know—a password or PIN and/or something you have—like a smartcard, a fingerprint, etc. Most of us use (or should use) passwords, but the system architecture supports tokens or biometrics through plugin APIs. OS X also supports the Kerberos network authentication protocol and Digital Certificates.

The operating system provides numerous run time protections. Applications are digitally signed to verify identity and integrity. Viruses don't do well in this environment.

Safari keeps a database of known fraudulent websites. The Mail application filters spam. Downloaded applications are quarantined and you need to approve them the first time you run them. XProtect maintains a profile of known malware and prevents download via many applications. A good argument for using Apple's apps!

In practical terms, Mac OS X is relatively immune from viral software because of features like sand-boxing, application signing, and library randomization. Malware attacks are currently more theoretical than real. They are a vulnerability, not a threat. The Mac isn't completely immune, but it's extremely safe.

All of this layered security is designed to be user-friendly. Most of the security is hands-off and non-intrusive. The OS provides only meaningful security alerts because bombarding the user with alerts and questions too frequently can lead to poor decision making and reflexive response. "Snow Leopard minimizes the number of security alerts that you see, so when you do see one, it gets your attention". [Security Configuration for Mac OS X Version 10.6 Snow Leopard (p23)] The firewall is application aware, providing protection without administration.

For those that require extra data protection, the OS offers a number of strong encryption options. A Keychain can store passwords, credit card numbers, or other secrets. If you need to protect files, they can be stored inside an Encrypted Disk Image created using Disk Utility. You can use Filevault to encrypt your entire Home Directory. Apple has announced that OS X 10.7 Lion will PROVIDE Whole-Disk Encryption which will protect applications and system files in addition to data and could provide a fast remote wipe of the drive via MobileMe. (This is speculation on my part, but assuming the encryption model is similar to that of iOS, it's a real possibility.)

Security is not a snapshot. Vulnerabilities in Mac OS X are frequently patched through Security Updates. We can expect to see improved security in Lion.

For more information about OS X security technology, or guides to "hardening" your computer, see the Dig Deeper section at the end of this article.

iOS Security

iOS was designed with security in mind. Everything is sand-boxed. Data Protection can be enabled on iOS 4 devices. This feature encrypts virtually everything on the device. Data Protection also allows for an immediate, remote secure wipe of the device using Find my iPhone or Exchange administration. Each file has its own unique encryption key. This is an opt-in service. Third party developers have access to the API. There is no back door to this encryption. "Security can only serve one master." Geddis.

If you have an iPhone, iPad or iPod Touch, you'll want to confirm that Data Protection is enabled on your device, particularly if it was upgraded from iOS 3. See Rich Mogul's TidBITS: Making Sure Your iOS Device is Really Encrypted (also published in the April issue of our newsletter)

Again, Dig Deeper suggests resources for further study.

What should I do?

First, you must determine your personal sweet spot on the continuum. A Mac is reasonably secure "out of the box." Hardening that security comes with trade-offs and should not be undertaken without understanding and due consideration. Be certain you know why and have a need before proceeding to do.

Your Password is the first line of defense. Use the Password Assistant to help choose or generate strong passwords. Your login password should be memorable, but still strong. Disable Automatic login on your Mac and consider the Display login Window as: Name and password option. Set a PIN or password for your iDevice. Use a Keychain or a third party solution to store unique, (random?,) strong passwords for all services and devices. Finally, the best answer to any "security question" is something different. For example, if my bank asks

me for my mother's maiden name my answer might be "Harry Potter" or, for that matter, "xdc@f89". Neither is something you're going to glean from reading my Facebook page. I log my answers to these questions in Password Wallet.

Many experts suggest logging in as a Standard User but my practice is to run as an Administrator. This is less secure but more convenient. Some software doesn't run very well for Standard Users. (Granted such software is poorly written, but that's of little consequence if you have to run it. [Yes, I'm looking at you Adobe.]) I am comfortable with this compromise. Your choice may be different and I'm okay with that. You have to weigh the risks against the rewards.

Physical security for your hardware is important and a Comprehensive Backup & Recovery plan is essential. Always practice safe browsing and email habits. Don't use software or media content from shady sources. Can you trust the torrent? If a security alert pops up asking you to vouch for an application, be sure you want to approve it. Did you download the application? Did you run it? Take a moment, read and consider the alert before you click Okay.

Run System & Software updates promptly. If you're of the "wait a week and see" club at least try to be aware of what vulnerability patches are provided by updates. (Apple doesn't always make this easy.) You must weigh the risks of the update against the risks of the threat. Generally, security patches are less likely to cause problems than OS updates (which in my experience are usually not problematic anyway.) If you use products like Adobe Flash keep them up-to-date too.

Anti-Virus software is a line-item on many security punch lists but my answer for most users is "no". At this time the costs—cpu cycles, stability, money—outweigh the benefits—primarily the identification of viruses that target Windows and the "classic" Mac environment. Anti-Virus software only protects against known threats anyway. The OS is relatively immune from viruses and Xprotect guards against malware. My position on this may change based on future threat profiles

Of course, Kaspersky and McAfee have white papers and blog posts explaining the shortcomings of XProtect. Both of these companies are also in the business of selling you scanning software and profile updates. I won't go so far as to accuse them of spreading FUD, but…

You should keep an eye on malware. Just because malware is largely a vulnerability at this point doesn't mean that it won't become a threat in the future. If the OS doesn't adequately address the threats (by patching vulnerabilities and profiling specific attacks) third party solutions may become necessary. Stay tuned.

The operating system is quite secure out of the box and, for most of us, doesn't need much tweaking, but there are some additional steps you can take to protect your data.

Secure containers are your friends. Know them. Use them. Love them. Examples include Keychains, Encrypted Disk Images, Password Wallet and 1password.

Setting a Firmware password prevents booting the computer from an alternative drive or in single user mode. I use this feature myself and recommend it to anyone whose computer might be subject to unauthorized access and tampering. This is a must for parents trusting Parental Controls. (Sorry folks, the bypass for the Parental Controls is on Google.) The downside is that if you lose the Firmware Password there is no back door. Be sure to store that password in a safe place. (The same is true for a Filevault master password)

Particularly sensitive certificates or passwords can be stored on a separate Keychain (file). This file can have tighter restrictions than your login Keychain. For example you can use a separate, (more secure?,) password and set the lock time to a very short interval. These extra Keychains can also be stored on a USB flash drive. [A tip from Geddis]. I don't feel the need to do this myself, but it's a safe and secure

way to use these certificates across multiple machines and having them separate from the computer adds an extra layer of security.

Remember, when it comes to hardening your system, consider the "expert" advice before implementing it. Is it right for you? (Again, understand "why" before "do".) Is the expert even speaking to you? For example, the NSA hardening guidelines are necessary for those protecting nuclear secrets, but some of these steps are complete overkill for most users (Geddis agrees with me on this) and may even cause problems. For example, Changing permissions on the home directory is more secure, but might screw something up down the road. Other users can only see the base level of your home directory anyhow, items in folders such as Documents are secure. Setting the firewall to "stealth" mode could be considered hostile by some network administrators and might get your access port closed down on some networks. If the firewall is working, are you really worried about a ping? Instead of hardening, use the OS as it was designed to be used and benefit from the protections it provides.

No computer will ever be 100% secure but Apple provides a secure foundation, and a number of easy-to-use tools to help you keep your data safe.

Dig Deeper

General Security

Several papers were referenced within the body of the article. All are relatively brief and accessible to lay-persons.

Wired: Threat Level provides news and information about security related topics.

Schneier on Security (SoS) is Bruce Schneier's blog covering security and security technology. SoS provides a steady diet of security food for thought. Schneier is very readable. His blog deserves a place on everyone's RSS feed list. Schneier also wrote a book by this title and is the author of several other books on the topic. The books are great if you prefer your information bound and organized, but most of the key points can pulled from the blog and essays on his website.

ZDNet's Zero Day Blog covers the latest in software/hardware security research, vulnerabilities, threats, and computer attacks. Their coverage includes Mac OS, iOS and social media exploits.

DC 612 is a local "hacker" spin off from the Las Vegas Defcon conference. A number of InfoSec professionals attend. It can be very geeky, but you needn't be put off by the "hacker" nomenclature. They meet monthly.

Mac OS

Light and fluffy overview: Apple - Mac OS X - Security

Mac OSX Security goes into a little more detail.

Mac OS X Security Configuration Guides provide an accessible technical introduction to the security architecture plus suggestions for hardening the system if warranted.

Apple's Developer Library:Security Overview provides a more in-depth look at Mac OS X (and iOS) security architecture.

NSA Fact sheet: Hardening Tips for Mac OS X 10.6 has some good information but remember that doing everything suggested here is overkill for most of us.

Way too much information: DISA Secure Technology Implementation Guide 10.5 Note that the 10.6 guide has yet to be published.

For the hard-core cryptopunk and/or InfoSec wonk (or those with insomnia): Apple FIPS Cryptographic Module, v1.0 FIPS 140–2 Non-Proprietary Security Policy

iOS

HT1766 iPhone and iPod touch: About backups is a KB article outlining what is backed up during an iOS device iTunes sync.

Apple's Security Overview also covers the iOS architecture.

Okay, it's not "reading" but you can geek out at iTunes U:WWDC 2010 Session 209: Securing Application Data (You will have to register for a free Apple Developer account.)

Jeff Berg; ACSP | Apple Certified Support Professional; Apple Consultants Network member | ACN; Minnetonka, MN (Twin Cities Metro); 781.350.0598

Where Has The Time Gone?

By Bruce Thompson

It is hard to believe but mini'app'les is almost 33 years old! The first written communication among Apple users is dated July 26, 1978. The first "official" edition of the newsletter (it says so right on the front page) was August, 1978. I thought it might be interesting to take a look back and see how things have changed (or not changed, as the case may be).

Remembering that at that time the Macintosh had yet to emerge, the newsletter focused on the Apple II. One article concentrated on the DOM (Disk Of the Month). These disks were sold at meetings for the basic cost of the disk. They typically contained a compilation of software games and utilities. Since modems were expensive and rare, members greatly appreciated the work of the Librarian in finding and compiling disks. Many of the programs were copied from disks provided by other user groups or organizations that specialized in Apple computer programs. This disk contained programs from the International Apple Core (IAC) and contained programs such as Jane's Egg Timer (a countdown timer), Spiral Demo, Alphabetize, Asteroyder (a space game from the Japan Baked Apple User Group), and Catalog Management, a program that "enables the running (etc.) of programs from the catalog with just a keypress or two". There were also several utilities / sub-routines targeted at the programmers in the group.

In addition to several programs (typed out so they could be typed into your Apple), there was a large chart of "PEEKS – POKES & CALLS", again programming information. The programming emphasis is shown by the Special Interest Groups (SIGs), such as Pascal, a Disk Programming Seminar, and a programming group that met in the Fort Snelling area.

Dan Buchler, the President at the time, reported on a meeting of representatives of the Twin Cities Micro Users groups, at which the 17 Presidents represented about 1000 local users. Groups represented were from 3M, Honeywell, and Univac user clubs, Apple, Heath, TRS-80, PET, and S-100 computer specific groups, the Minnesota Computer Society, and some others. Dan also reported on a couple of printers of the era; the DIP-84 cost $595, the Epson MX-80 was $650! And then you needed an interface card to connect either one to your computer. "Plug and Play" was still a long way off.

Finally, in the news of the day, there were rumors about some problems with the Apple III. Apparently the chip sockets were "too loose", as chips were falling out or losing contact and there was a problem with the Clock Calendar chip that did not meet specifications. Apple provided a rebate of $50 for customers that had bought the III with the faulty chip. Things have certainly changed a bit since then.

Apple User Group Bulletin - April 18, 2011

Recent Highlights from the Apple User Group Resources website:
http://appleusergroupresources.com

- NCMUG: Supporting Relief Efforts in Japan
- RL Graeme Moffatt: Christchurch Earthquake Relief
- Bob "Dr. Mac" LeVitus: Mid-Atlantic User Group Tour
- SF Cutters: Las Vegas SuperMeet Mystery Guest
- Upper Keys Macintosh User Group: iPads and More
- MacCamp: OMUG's Movie Trailer and Reference Page
- PMUG Hosts MacCamp Spring 2011: April 15-17
- Vintage Computer Festival East: 7.0

- Denver Apple Pi: Jeff Gamet of the MacObserver Presents
- Offers for User Group Leaders and Members including:

• Special Offer – ThinSkin for iPhone 4: 50-66% Discount
• Special Offer – Boom Volume Booster: 45% Discount
• Special Offer – Disk Drill data recovery: 30% off
• Special Offer – SSERO Defender iPad protector: 20% Discount
• Special Offer – Mac|Life: 75% Off
• Special Offer – O'Reilly: Discounts for User Group Members

Is Apple Using Your iPhone to Track You?

by Jeff Berg

You've probably seen a similar headline to the one atop this story, or maybe heard this question posed as a teaser for a sensationalist news segment. Betteridge's Law applies: *Any headline that ends in a question mark can be answered by the word* ***no***. No one, particularly Apple, is tracking you and the real story is less sensational. Andy Ihnatko provides a rational perspective. If you only read one story about this controversy (or *non-troversy*), I recommend Ihnatko's *Hey, wonderful: there's a location-tracking file on my iPhone*.

The Story

Security researchers Alasdair Allan and Pete Warden reported the "discovery" of a "secret" file on iPhones (and 3G iPads).[*Got an iPhone or 3G iPad? Apple is recording your moves*] The file, *consolidated.db*, is a timestamped database of your approximate position based on cell-towers and wifi access points. The unencrypted file is stored on your iPhone, and is also a part of the backup file on your computer. There is no evidence that this information is being secretly transmitted to Apple and, in fact, such a transmission would be a violation of California law.

The file may be part of the *anonymous diagnostic and usage information* sent to Apple if you consent to share it. (Instructions to opt-out are included below.)

John Gruber reports *consolidated.db* is used by iOS *Location Services* to provide an estimate of position. These estimates are often close enough that *Location Services* doesn't need to use the GPS radio. If a GPS fix is required, a precise position can be determined more quickly. This provides a better user experience through less waiting time and better battery life.

There is nothing ominous about the existence of the file, but the historical cache of the information is a minor concern. Gruber reports that the historical persistence of the data is probably due to a bug or an oversight, and Apple will most likely fix the problem with an update. The cached data will be flushed so that only the most recent location data will be present.

Alex Levinson, an Information Security Engineer and author of a book on iOS forensics, is critical of the Allan-Warden report. [*3 Major Issues with the Latest iPhone Tracking "Discovery"*] Levinson reports that *consolidated.db* is neither new, nor secret. The iPhone has been recording this information prior to iOS 4 but when Apple opened the *Location Services* API to third-party developers, allowing their software to use location information, the file had to be moved to an unencrypted area. Levinson wrote a followup piece with more information about *Location Services* and mobile information security. [*3 New Thoughts on Mobile Location – A Follow up to Apple Location Tracking*]

What Should You Do?

First, do nothing. The information is only stored locally, isn't particularly sensitive (though I suppose it could be potentially embarrassing to some), and there is very little risk. This is a *vulnerability*, not a

threat. (See ***Security: Mac OS, iOS and You*** in this issue.) A burglar or stalker using *consolidated.db* is a *movie plot threat*. Even if you are targeted, there are easier ways of tracking you—for example, they can follow you. The *What about the children?* concern, raised by Al Franken and others, is also far-fetched. A visit to the local mall, or *Facebook*, is more of a threat than location history on the phone. Some cell phone carriers offer the tracking of children as a **service** to parents. If the government or law enforcement wants this information, and can convince a judge they have just cause, they will get a warrant for the cell phone records that your network provider keeps. I'll confess that I am disturbed by the news coming out of Michigan that police are downloading information from phones during routine traffic stops [Google it, too many references to pick a citation], but I see this as an overall civil rights issue, not a problem particular to *consolidated.db*. If they get stuff on my phone, my location history is of minor consequence.

Use a PIN or password for your device and set the lock time to a reasonable interval. I set my iPhone to lock after five minutes but use a longer period for the iPad—unless I'm in an Airport or other "risky" public place. If I'm out and about, and fear the device might be at a higher risk of theft, I reduce the time-to-lock to five minutes. (That setting is not cast in concrete!)

Enable data protection on your device. (See ***Security: Mac OS, iOS and You***)

If your device does disappear, use MobileMe's (free) *Find My iPhone* service to locate it. If you feel you have cause, erase the device. Because the *consolidated.db* file is unencrypted, I am not 100% positive that it would be erased. However, erasing the rest of the information on the device will help to insure your anonymity. If you're worried about wiping your device, you're not backing up often enough.

If your device is jailbroken, be sure to change the root password to something other than the default. My main objection to jailbreaking is that it presents a security risk.

Encrypt the device backup files on your computer. This is trivial to do, it's a check box in iTunes. (Be sure to store the password in a safe place.) Also make sure your computer is password protected. (Again, ***Security: Mac OS, iOS and You*** has more information.)

If you've previously opted-in to share *anonymous diagnostic and use information* with Apple and want to stop doing so, reset warnings for your device(s) in iTunes. Connect your iPhone or iPad to your computer. Right (CTL) -click on the device in the list that appears in the left column. Choose **Reset Warnings** from the pop-up menu. The next time you sync your device a dialog box asking you to share this information will appear. Click disagree. (I continue to share this information myself because I want the iOS and network to improve and don't find the information to be sensitive.)

Keep Calm and Carry On

Apple made a mistake and probably owes us an apology. The contents of *consolidated.db* should be flushed periodically, keeping only the data that is useful for *Location Services*. The reality is, however, that the information isn't particularly compromising—unless you've been sneaking off to Florida and not telling your spouse. In the absence of evidence to the contrary, I attribute this to error, or incompetence, not malice. [*Hanlon's razor*]. If Apple doesn't fix the problem in a timely manner, we have cause for complaint. But, for the moment we should *Keep Calm and Carry On*.

Apple's response.

Jeff Berg; ACSP | Apple Certified Support Professional; Apple Consultants Network member | ACN; Minnetonka, MN (Twin Cities Metro); 781.350.0598

TidBITS April Watchlist:

by TidBITS Staff

GraphicConverter 7.2 -- Lemkesoft has released GraphicConverter 7.2. Among the many new features are a command to Select Last Selection, additional movie options for batch conversions,

WebP import and export, Apple-Touch-Icon export support, and an option to cycle through open windows. Full release notes are available at Lemkesoft's site. (Free update, $39.95 new, 100 MB).

Boot Camp 3.2 Update for MacBook Pro (early 2011) -- According to Apple, Boot Camp 3.2 Update corrects just a few issues for 2011 MacBook Pros. The update addresses issues with shutdown, along with Japanese and Korean keyboards on those Macs when running Windows 7 via Boot Camp. (Free, 21.55 MB)

ChronoSync 4.2/ChronoAgent 1.2 -- Econ Technologies has released ChronoSync 4.2 and ChronoAgent 1.2. Among the new features in these versions of the synchronization/backup software are new Trial Sync options, including additional file statistics, time estimates, and options for controlling and comparing files on both sides of the sync. Also, Econ Technologies enhanced scheduling options with Retry on Errors, which runs a sync again if errors occurred, and Sync Limits, which limits the number of syncs that can take place simultaneously to prevent too many from happening when a Mac rejoins a network. ChronoAgent also adds the capability to schedule ChronoSync Container Documents using the Sync When Available option. Full release notes for ChronoSync and ChronoAgent are available. ($40 new for ChronoSync, $10 new for ChronoAgent; free updates; 21 MB, 3.2 MB)

Dropbox 1.0.28 -- Perennial TidBITS favorite Dropbox has been updated to version 1.0.28. The minor release fixes a rare crash and includes a few other unspecified small tweaks. We tend to find that Dropbox fails to auto-update itself as it should, and indeed, it didn't do so for me, so I downloaded and installed manually. You can check which version of Dropbox you're running by hovering your mouse pointer over the Dropbox menu bar icon, or by clicking the icon, choosing Preferences, and then checking the Account tab. (Free, 21.6 MB)

Mac OS X v10.6.7 Supplemental Update for 13-inch MacBook Air -- Apple has released a rare Supplemental Update for Mac OS X 10.6.7, exclusively for the most recent edition of the 13-inch MacBook Air. The update addresses an issue that makes the system unresponsive when using iTunes, and Apple recommends it for all applicable MacBook Air users. The Supplemental Update is available via Software Update, or directly from Apple's Web site. (Free update, 461 KB)

GarageBand 6.0.2 -- Apple has released a minor update to the Mac version of GarageBand. Version 6.0.2 reportedly improves overall stability, but most notably it introduces support for opening projects created in the iPad version of GarageBand (see "GarageBand for iPad and Mac Not Yet Ready to Play Together," 11 March 2011). When you first open an iPad project after installing this update, GarageBand on your Mac will need to download an additional update that's just shy of 200 MB. Note also that when you open iPad GarageBand projects, you'll immediately be prompted to save them under a new name. That's because once you've modified a project in the desktop edition, it can no longer be opened by GarageBand for iPad. ($14.99 new on the Mac App Store, free update, 47.44 MB)

LogMeIn Ignition 2.0.264 -- We generally restrict the TidBITS Watchlist to Mac software, but the 2.0.264 release of LogMeIn Ignition is worth a shout because of how it integrates with the Mac. This update to the iOS remote screen control app adds remote file browsing to its bag of tricks. LogMeIn requires a free account, and then a free or paid installation of software on the Macs or Windows systems you want to control. Ignition's update lets you browse through files, copy them to your device, view them (if in one of iOS's supported formats), and print them. You can also transfer files between two computers in your LogMeIn account using the app. ($29.95 new, free update, 9.8 MB)

Things 1.4.5 -- The folks at Cultured Code have crossed releasing Things 1.4.5 off their to-do list. New to the task-management utility is support for the Things URI scheme, which was previously offered only in the Things iOS apps. The Task Modification Date is now available by AppleScript. Among the numerous bugs fixed are an issue where

items could reorder themselves after syncing, an issue where marking items complete from within search results would bounce you to the Inbox, issues with grouping and sorting of tasks and projects, various issues with recurring tasks, and a crash under Mac OS X 10.4. ($49.95 new, free update, 8.0 MB)

Skype 5.1.0.914 -- Version 5.1.0.914 of the voice-over-IP application Skype restores a feature that had gone missing: highlighting the name of the current speaker in group calls. Also included in this release is the capability to select recently called numbers from the dial pad. Skype also says that several minor bugs are fixed, including a webcam detection issue. (Free, 20.2 MB)

NoteBook 3.0.9 -- Circus Ponies has released NoteBook 3.0.9. The update to the note-taking and text-collection utility fixes many issues, including a crashing bug when saving a notebook with pages open in separate windows, and another crasher related to iCal syncing. Other bugs fixed include issues with text selection, problems with the Spotlight importer, an issue with undoing shape changes, a few small memory leaks, a problem with sticky flags, and a flaw with the Find panel. ($49.95 new, free update, free trial available)

PDFpen and PDFpenPro 5.2.2 -- Smile has released PDFpen and PDFpenPro version 5.2.2, adding the capability to choose the destination for files when you scan them in. Numerous fixes, including one for an OCR-related hang, are also included. There's now full Japanese help text, too. ($59.95 new, free update, $25 upgrade, 41 MB)

Aperture 3.1.2 -- Photographers thinking about switching from iPhoto to Aperture take note: Apple has released Aperture 3.1.2. In addition to improving the software's overall stability and performance, the update addresses numerous issues with importing photographs from iPhoto — including at least one that could cause Aperture to crash. Various other importing issues are addressed, too. Also fixed are bugs with reference images, switching between libraries, hangs while using brushes, crashes with Retouch, and compatibility problems with XMP Sidecar files. Mac App Store purchasers should, of course, update the software via the store. ($79.99 in the Mac App Store, free update; 578 MB from the Mac App Store, 297.63 MB for the standalone updater from Apple's Web site)

MarsEdit 3.2 -- Red Sweater Software's blogging tool MarsEdit has reached version 3.2, with several new features to show for it. A running word count now appears in the post status bar, WordPress tags are handled better, and malformed XML and "bad characters" no longer trip up the software. Performance for both the media browser and the autosave feature is improved, too. Numerous bugs are fixed, including issues with Convert Line Breaks, an issue with lost formatting for image attachments, and the reliability of Paste HTML Source. Several crashes have also been eliminated. ($39.95 new, free update, 6.2 MB)

Firefox 4 -- Mozilla has released Firefox 4. The upgrade sports a revamped user interface and runs atop the Gecko 2.0 engine. According to Mozilla, that means it's up to six times faster at running JavaScript than the previous version of the browser, and now offers vastly improved support for HTML5 and CSS3. Firefox now supports the Do Not Track header, enables Firefox Sync by default, supports Google's WebM video format, and handles plug-in crashes more gracefully. Lengthy release notes are available at Mozilla's Web site. (Free, 26.8 MB)

Sparrow 1.1 -- iOS-inspired email software Sparrow has been updated to version 1.1. Starting with this incarnation of the software, Sparrow now supports many more types of email accounts; in addition to Gmail, you can now use the software with MobileMe, Yahoo!, AOL, and any IMAP account. Also new is support for Gmail's Priority Inbox feature, an Unread View, per-account signatures, and a formatting bar for composing richer messages. Sparrow now offers support for multitouch gestures, contact groups, and Gravatars, too. In addition, close to two dozen bugs have been fixed. ($9.99 via the Mac App Store, free update, free lite version available, 10.2 MB)

Skitch 1.0.4 -- Screenshot sharers should shout in celebration, though they shouldn't try saying that

three times fast. Skitch has been bumped to version 1.0.4, and its most notable new feature is that it no longer requires that you create a skitch.com account in order to use the software. Other improvements include a simplified Welcome screen, and a fix for a crash affecting some 10.6.6 users. (Free, 6.5 MB)

Hot Links Of The Month:
Compiled by Tom Ostertag

Apple, Inc.

Apple Reports Second Quarter Results **| *Apple Hot News***

Apple co-founder Steve Wozniak open to returning to company if asked **| *AppleInsider***

Mac Software

Apple releases iTunes 10.2.2 update to fix minor bugs **| *AppleInsider***

Apple issues update for Mac OS X 10.7 Lion Preview 2 **| *AppleInsider***

Inside Mac OS X 10.7: Apple to strip most Aqua gloss **| *AppleInsider***

Apple's Final Cut Pro update rumored to add iPad, Thunderbolt support **| *AppleInsider***

Microsoft Office for Mac 2011 SP1 (14.1) **| *Tidbits***

PDFpen and PDFpenPro 5.2.4 **| *Tidbits***

Apple Previews Final Cut Pro X: New, Faster, and Cheaper **| *Tidbits***

Microsoft Word 5.1 Returns... to the iPad **| *Tidbits***

Free OmmWriter Dana Creates a Tranquil, Non-Distracting Writing Environment **| *Low End Mac***

Mac Hardware

Last-Gen iMac Supplies Dry Up As Apple Prepares New Sandy Bridge Thunderbolt IMacs **| *Cult Of Mac***

Intel Will Support USB 3 Alongside Thunderbolt **| *Edible Apple***

iPad

iPad 2 for Travel **| *Apple Hot News***

GarageBand for iPad: Music Talent Not Required **| *Apple Hot News***

Apple releases iOS 4.3.2 with fixes for FaceTime, 3G connectivity **| *AppleInsider***

85% Of All Tablets Are iPads **| *Cult Of Mac***

iPod/iPhone/iTunes

Verizon announces 2.2M activations of Apple's iPhone in Q1 2011 **| *AppleInsider***

Miscellaneous

Keep Your Mac Mac Running Like A Mean Machine [Video How-To] **| *Cult Of Mac***

iLounge + Mac launches, spotlighting cool new Mac products **| *iLounge***

Skype 5 for Mac: A Huge Step Backward **| *Tidbits***

Undelete From Trash To Original Locations **| *Mac OS X Hints***

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 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	Dave Diamont 952-232-8868 ddiamont@mac.com
Secretary	Joel Gerdeen 763-607-0906 jgerdeen@mac.com
Treasurer	Dave Lundin 715-483-3776 cdlundin@centurytel.net
Membership Director	Les Anderson 651-735-3953 anderslc@usfamily.net
Publications Director	Tom Ostertag 651-488-9979 tostertag@usfamily.net
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