

printout

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

New Technology

Our resident tech guru, Tom Owad, will give us his take on Apple's new technology. Apple has just released new laptops, new iPads, the new Thunderbolt (I/O technology that supports high-resolution displays and high-performance data devices through a single, compact port), and coming soon: iOS 4.3 for your iPad, iPod touch, and iPhone and OS 10.7 Lion. There's gotta be something for everyone.



Meet us at

Giant Food

Corner of Trindle Road & 32nd St (Route 15)
3301 East Trindle Road, Camp Hill, PA 17011

Tuesday, March 15, 2010, 6:30 p.m.

Attendance is free and open to all interested persons.

Contents

New Technology	1
Keystone MacCentral Minutes <i>by Gary Brandt, Recorder</i>	3
Verizon Wireless Sets iPhone Plans and Throttles Data <i>by Glenn Fleishman</i>	4
Meeting Schedule for 2011	4
Apple Reveals More about OS X Lion <i>by Adam C. Engst</i>	5
Secrets of Thunderbolt and Lion <i>by Glenn Fleishman</i>	6 - 7
Apple's Security Past Defines Its Future <i>by Rich Mogull</i>	7 - 9
March Software Review <i>by Tim Sullivan</i>	9 - 10
Mac 911 <i>by Christopher Breen</i>	11 - 13

Keystone MacCentral is a not-for-profit group of Macintosh enthusiasts who generally meet the third Tuesday of every month to exchange information, participate in question-and-answer sessions, view product demonstrations, and obtain resource materials that will help them get the most out of their computer systems. Meetings are free and open to the public. The *Keystone MacCentral Printout* is the official newsletter of Keystone MacCentral and an independent publication not affiliated or otherwise associated with or sponsored or sanctioned by any for-profit organization, including Apple Computer, Inc. Copyright © 2011, Keystone MacCentral, 305 Somerset Drive, Shiresmanstown, PA 17011.

Nonprofit user groups may reproduce articles from the Printout only if the copyright notice is included, the articles have not been edited, are clearly attributed to the original author and to the Keystone MacCentral Printout, and a copy of the publication is mailed to the editor of this newsletter.

The opinions, statements, positions, and views stated herein are those of the author(s) or publisher and are not intended to be the opinions, statements, positions, or views of Apple Computer, Inc.

Throughout this publication, trademarked names are used. Rather than include a trademark symbol in every occurrence of a trademarked name, we are using the trademarked names only for editorial purposes and to the benefit of the trademark owner with no intent of trademark infringement.

Board of Directors

President

Linda J Cober

Vice President

Tom Owad

Recorder

Gary Brandt

Treasurer

Ron Rankin

Program Director

Gary Brandt

Membership Chair

Eric Adams

Correspondence Secretary

Sandra Cober

Newsletter Editor

Tim Sullivan

Industry Liaison

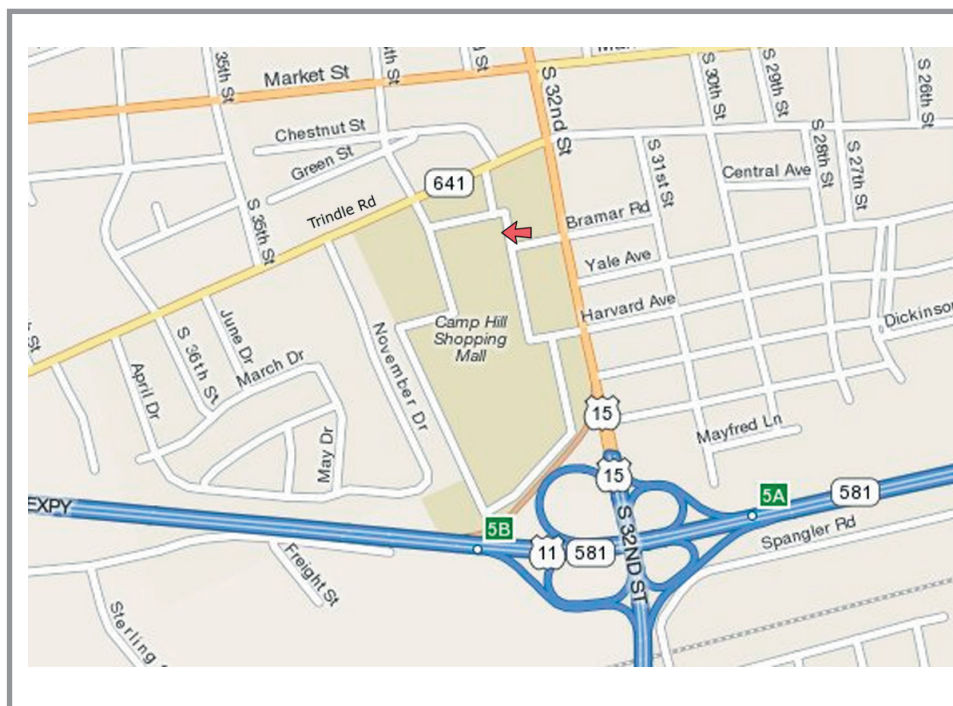
Wendy Adams

Web Master

Tom Bank II

Librarian

Tim Sullivan



Keystone MacCentral Essentials

Meeting Place

Giant Food (upstairs)
Corner of Trindle Road & 32nd St
(Route 15)
Camp Hill

Web Site

<http://www.keystonemac.com>

Mailing Address

310 Somerset Drive
Shiresmanstown, PA 17011

Keystone MacCentral

Minutes

February 22, 2011

Business Meeting

President Linda Cober brought the meeting to order and asked board members for their reports. Eric Adams told us he had found a list of Macworld vendors that would be added to the list of vendors he contacts for donations for our auction.

Ron Rankin reported that he had purchased training videos on iPhoto '11 and iMovie '11 and that he had a short video on Address Book. Linda told us she would not be at the March meeting.

Linda mentioned the Groupon web site and its daily deals. This site offers deals for local products and services. Linda would get a credit from them if you let her sign you up. Eric and Wendy Adams are also Groupon members. Tanga is a similar site offering deals.

Q&A & Comments

The first question was about changing WMA music files from a PC to music files that could be added to iTunes on a Mac. Jim Carey suggested re-ripping the CDs on the Mac and mentioned that this process is pretty quick on newer Macs. We looked online for conversion programs and found a number listed. We tried the App Store and found some there that should work.

Tim Sullivan asked about using an iPad to replace his five remote controls. The App Store lists some applications for TV remotes, although we found out that one of them was a joke application. Logitech makes a Harmony remote that is said to work with over 225,00 devices. Verizon has a remote application that lets you control your DVR with remote devices.

Program Notes

The February program on Facebook was presented by Eric and Wendy Adams. Eric had set up an account to check out Facebook. He thought Wendy might like it so he showed her how it worked and she has since become hooked. Facebook

will prompt you for some personal information and will then suggest people you might know based on that information. Some of these suggestions are based on mutual friends you might have with someone else. You would send a friend request to people you want to contact and they can choose to accept or deny that request. Businesses have also adopted Facebook so their customers can follow them.

Eric logged into his account to show us how things work. From your home page you can see a listing of your friends currently online. Click on a link from that list to see what they are up to and what they have posted.

Eric showed us how to edit Facebook's account settings. Privacy options can be set to allow everyone to see your posts or more narrowly to allow only your friends to see posts. You will see a window of customized ads on your Facebook page. These are based on your profile information and your interests.

Wendy logged into her account to demonstrate how she uses Facebook. Wendy has posted many photos to her page. These photos can be tagged with your friends' names. These tags are placed on a particular spot on the picture and rolling over the photo will display the tagged names.

A lot of content on the internet has a Like button that automatically posts a link to that content on your Facebook page. If you are a friend of Wendy you can quickly click on those links to see what Wendy likes. You can be selective viewing what your friends post if there are topics that don't interest you. You can limit showing posts based on keywords. Groups can be set up on Facebook. Wendy has one set up for the Brownies troupe she leads. There is also a Facebook application available for the iPhone, although with some limitations. ☹



Verizon Wireless Sets iPhone Plans and Throttles Data

Verizon Wireless will [charge \\$30 per month](#) for a so-called “unlimited” data plan paired with the new iPhone 4 Apple designed to be compatible with Verizon’s CDMA network. However, Verizon also published a [terms and services document](#) that explains that [it may downsample and transcode media](#), as well as throttle the network’s heaviest users.

The “unlimited” plan is the only data offering from Verizon, which made it clear this would be a limited-time offer, as well. Afterwards, the company is likely to switch to a two-tiered service much like it and AT&T offer for all other phones. In June 2010, AT&T switched to a \$15-per-month 200 MB DataPlus plan and \$25-per-month 2 GB DataPro plan for new subscribers and those who changed service plans.

Verizon also set the price for its iPhone 4’s Personal Hotspot feature at \$20 per month with a separately metered 2 GB of service included, as it offers with other smartphones. Extra data usage costs \$20 for each gigabyte used within the billing period. (See [“AT&T Changes Tethering to Mobile Hotspot,”](#) 2 February 2011, for details about AT&T’s upcoming mobile hotspot offering, still not yet announced for the iPhone.)

Verizon’s two bandwidth-reducing strategies may irk some users. “Optimizing” and “transcoding” refer to downsampling image data, such as making a JPEG image less faithful to the original, or degrading the quality of video (which can introduce jerkiness and artifacting) to reduce the bandwidth consumed in sending it. Technically, neither would be a violation of net neutrality principles, because it’s being called a network management strategy instead of a discriminatory method to show images or video from Verizon properties or partners better than that from other parties.

The throttling may be a bigger problem. Mobile carriers all reserve the right to impose limits or pull the plug on people they believe are violating reasonable usage policies. Carriers’ fine print often says that mobile can only be used for e-mail, Web surfing, and intranet use, despite the fact that smartphones handle a million other tasks. And there are certainly network abusers, who use phones to run Web servers or stream video 20 hours a day. Verizon says it’s looking at just its 95th percentile users, but that would sweep in an awful large number of people. Comcast, with whom I have spoken many times about its 250 GB cap on usage each month for cable broadband, finds less than 1 percent of its users have problematic consumption, and of

those, many have compromised computers used for the distribution of pirated media or as zombie agents of malefactors.

Verizon Wireless and other carriers have a history of enforcing policies in ways that make sense internally, but not to customers. Without clear guidelines as to what will trigger throttling—such as a particular amount of data consumed in a 1-hour or 24-hour period, or use of services by a subscriber that Verizon contends aren’t allowed—and without warnings that specifically address behavior Verizon will disallow, the company may face scrutiny from Congress, legal action from affected customers, and regulatory enforcement attempts.

For now, Verizon [told public-radio program Marketplace](#) (on which you’ll hear yours truly, too), it doesn’t have plans to engage throttling. It just wants the option available for reasons that a spokesperson was unable to articulate clearly. ☹

Meeting Schedule for 2011

Other groups have first call on the meeting rooms at Giant. Therefore our schedule must be a bit flexible. These are the dates for the remaining meetings in 2011:

3/15 - 3rd Tuesday

4/26 - 4th Tuesday

5/17 - 3rd Tuesday

9/20 - 3rd Tuesday

10/25 - 4th Tuesday

11/15 - 3rd Tuesday

12/20 - 3rd Tuesday

Apple Reveals More about OS X Lion

Apple has announced the first developer preview of OS X Lion, still eschewing the expected 10.7 version number but revealing a few more features and sticking to the summer ship date promise. For details on what Apple previously announced about Lion, see [“Apple Offers a Glimpse of OS X Lion”](#) (20 October 2010).

In the press release, Apple makes much of the previously announced features, such as Launchpad, Mission Control, full-screen mode, gestures, Auto Save, and the capability for applications to resume where they left off. But at the end of the press release, Apple reveals some previously unknown improvements slated to appear in Lion. They include the following:

- Apple Mail 5 will include a widescreen layout reminiscent of the iPad Mail app that I’ll bet will run in full-screen mode. Also, taking a page from Google’s Gmail, Mail will feature Conversations, which automatically groups related messages into an easy-to-read timeline, even if the subject changes along the way. Apple also claims that Mail will have more-powerful searching capabilities and support for Microsoft Exchange 2010.
- A new Finder feature called AirDrop will make it easier to copy files wirelessly from one Mac to another with no setup, discovering local Macs automatically. Click the AirDrop icon in a Finder window’s sidebar to display nearby Macs using AirDrop, complete with photos for people in Address Book. To copy a file, drag it to the person’s name to copy it to their Downloads folder. Various utilities have offered features like this for years; AirDrop will have to outdo not just them, but the popular Dropbox.
- Auto Save didn’t sound like much when Apple first announced it back in October, but additional details now indicate that it will save changes in the working document rather than make additional copies. To prevent changes from being saved inadvertently, you can enable a lock feature, and Auto Save automatically locks documents after two weeks (when you might just be referring to the document, or would save any changes intentionally). Applications will have to support Auto Save explicitly.
- Another new technology, called Versions, will bring version control to the operating system, automatically saving successive versions of documents and providing an easy way to browse, edit, and revert to previous versions. No mention was made of any way of comparing versions automatically, though perhaps that will be an opportunity for independent developers. Versions will use an interface similar to Time Machine, though I hope it’s significantly snappier, since my experience is that browsing Time

Machine is a slow and often frustrating experience. As with Auto Save, applications will have to support Versions explicitly.

- Apple is promising an “all new FileVault” that provides full-disk encryption for local and external drives, along with the capability to wipe data from your Mac instantaneously. That’s one to let the security experts test carefully before using, based on FileVault’s past performance and the danger of a small bug causing entire disks to become inaccessible. For more on full-disk encryption, see Joe Kissell’s articles on PGP Whole Disk Encryption: [“Securing Your Disks with PGP Whole Disk Encryption”](#) (31 October 2008), [“PGP Whole Disk Encryption and PGP Desktop Professional 10.0”](#) (14 May 2010), and [“Whole Disk Encryption, and Why OS X 10.6.5 Broke PGP WDE”](#) (14 November 2010).
- Finally, despite Apple’s dropping of the Xserve line (see [“A Eulogy for the Xserve: May It Rack in Peace,”](#) 8 November 2010), OS X Server will make the transition to Lion, with Apple promising that the new version will make setting up a server easier than ever. That’s in part because Lion Server will be built directly into Lion, with software that guides you through configuring the Mac as a server. Also, a new Profile Manager will add support for setting up and managing OS X Lion, iPhone, iPad, and iPod touch devices. Wiki Server 3 will offer improved navigation and a new Page Editor. And Lion Server’s WebDAV support will provide iPad users the ability to access, copy, and share server-based documents.

Additional features will no doubt start to come to light as developers get their hands on the Lion preview. Interestingly, the preview is available to Mac Developer Program members through the Mac App Store, raising the possibility that perhaps we’ll all end up getting the release version of Lion through the Mac App Store as well. ☞



Secrets of Thunderbolt and Lion

You can read a thousand articles about the new Thunderbolt input/output technology in Apple's latest revision to MacBook Pro laptops, and the new revelations from Apple about OS X Lion. But via Twitter, I discovered that many people are unaware of or concerned about certain features close to their hearts. From online sources and a briefing with Apple last week, I can provide some reassurance and additional details.



These seem to be among the least well understood and documented items about Thunderbolt and Lion.

Thunderbolt's Blasts — Thunderbolt is a fascinating mix of old and new:

- Despite what the tech spec pages say, [Thunderbolt](#) actually has up to 20 Gbps available in each direction (full duplex), not 10 Gbps. While the Thunderbolt specification talks about 10 Gbps to and from a host, there are actually two channels over the same cable: one dedicated to DisplayPort for video, and the other for PCI Express data. Apple and Intel are likely sticking with the 10 Gbps rating because if you measured the throughput to a hard drive, for example, it would never go over 10 Gbps thanks to using only the PCI Express channel.
 - This dual-channel approach would let you run two high-resolution displays (which require bandwidth in the gigabits-per-second range) and a super-fast RAID drive (demonstrated by Promise Technology) or multiple drives that can work at full speed. On the new MacBook Pros, Thunderbolt manages both the internal screen and an optional external display, which is why you can't drive two external displays. On a future Mac Pro or Mac mini that wouldn't be an issue, nor would it be a limitation on a future iMac, as long as the iMac provided multiple Thunderbolt ports.
 - Because Thunderbolt provides two channels on the same cable, a display or hard drive can be in the middle of the daisy-chain without interrupting the flow of the other channel.
 - [Target Disk Mode](#) is supported under Thunderbolt. Until now, this mode worked only over FireWire connections.
- When a Mac is booted in Target Disk Mode, it acts as a hard drive for another connected Mac.
- You won't be able to boot a Mac from a Thunderbolt-connected drive for now, unlike with USB and FireWire. Andy Ihnatko has this [factoid](#), and I tend to trust him. I will be surprised if this isn't added later. We need a way to boot from external drives, and if Thunderbolt eventually takes over from FireWire, then it has to boot Macs, too.
 - If all you're connecting to a Thunderbolt port is a display, you can use an existing DisplayPort cable. The Thunderbolt controller automatically adjusts the signal output to be correct for DisplayPort-native ports on the other end. Thunderbolt data devices, such as hard drives, need to be connected with Thunderbolt cables. This means you can't put any Thunderbolt data devices downstream from a display connected via a DisplayPort cable; such displays would have to go at the end of the Thunderbolt daisy-chain.
 - The Thunderbolt port carries 10 watts of power, a significant amount for powering drives and other peripherals (though nowhere near enough to drive a large external display). Apple's hardware with a single FireWire 400 or 800 port (or one of each) can [deliver 7 watts](#) to the bus. USB 2.0 can push out a maximum of 2.5 watts, while USB 3.0 can hit 4.5 watts. Apple's high-power USB 2.0 can [generate 5.5 watts](#), which is enough to charge an iPad while it's plugged in and in use. Thunderbolt devices can also boost power downstream: an AC-powered display could push 10 watts out the port on the "far" side from the computer in the daisy-chain. (Apple's external iPad USB-to-AC charger is rated at 10 watts, but it's just a USB plug connected to power, not a data connection.)
 - Thunderbolt will allow splitters and other baroque configurations of adapters, Apple told me. For instance, you could have a DisplayPort adapter with two Thunderbolt ports for daisy-chaining. Apple has no plans to discuss here, but there's clearly room for a robust market of cables, hubs, adapters, and other elements to make it easier to use legacy video standards.
 - It should be possible to build Thunderbolt-to-eSATA and Thunderbolt-to-FireWire adapters that enable connectivity with older gear that you already own. It's also possible that we'll see Thunderbolt-to-USB 3.0 adapters, though it probably doesn't make much sense to convert between Thunderbolt and USB 2.0 given the low cost and ubiquity of USB 2.0 parts. A company could create a dock-like device that would plug into a Mac via Thunderbolt and provide a slew of USB, FireWire, eSATA, and other ports.

Lion's Roars — We have to keep mum on many Lion details, as many of us at TidBITS are enrolled in the

developer program that gives us access to non-public preview details. However, on the public side:

- Lion's [AirDrop](#) will let you exchange files between two Macs (and, one expects, iOS 5) using Wi-Fi. But it's not a variant on Bonjour: the two Macs do not need to be connected to the same Wi-Fi base station or larger Wi-Fi network. Rather, they only need to be within Wi-Fi range of one another. AirDrop uses a peer-to-peer ad hoc connection, though one that's instant to set up and secure. A Mac using AirDrop doesn't drop a Wi-Fi network connection if it has one; it can communicate to another Mac and maintain its network connection, too. This requires newer hardware. I suspect nearly all machines shipped since 2007 or 2008 will have the right Wi-Fi gear, but Apple will need to provide more details as Lion's release date gets closer.
- Lion's FileVault is an entirely new bit of technology labeled with the old name. FileVault before Lion encrypted only the user's Home directory and was awkward in everyday

use. The new FileVault is a [full-disk encryption method](#): everything on the hard drive (and it seems, external drives, if you wish) is completely secured. Apple didn't explain whether you will need to enter a password at boot, as is the case with many existing full-disk encryption products for OS X, Windows, and Linux. You may also be able to wipe a FileVault-protected Lion system remotely. Apple told me that the new MacBook Pro models will use accelerated encryption processing in the i5 and i7 processors to eliminate any performance loss due to handling encryption.

- OS X Server is built into Lion, although it apparently will not be active when you upgrade or boot a new machine. Apple declined to provide details, but said that reports that you had to make a choice during installation of Lion, or reinstall Lion to use server features, were inaccurate. You will have to activate something within Lion, though what form that will take, or if it will be available for free remains unknown. I wouldn't be surprised if you would pay for the upgrade in the Mac App Store in some way. ☹

by Rich Mogull

Apple's Security Past Defines Its Future

It's a foundational meme of the modern Internet that once Apple's market share rises above a certain nebulous level, Mac users will face a horde of viruses, worms, and other nefarious malware that will quickly burst our bubble of innocence and drag us into the swamps of despair long populated by our Windows-using brethren. But while market share is clearly an important factor in the relative security of the different platforms, and probably the most significant one from a historical perspective, such arguments fail to account for the current threat environment surrounding both Apple's products and the Internet at large.

Recent moves by Apple, especially the hiring of prominent security experts like [David Rice](#) (the author of "[Geekonomics: The Real Cost of Insecure Software](#)") and Window Snyder (former head of security for Firefox maker Mozilla), combined with frequent product updates, indicate that Apple may be quietly, yet significantly, improving their security infrastructure. With Apple's rising popularity, increasing use in the enterprise, and dominance in mobile computing, such moves could help the company avoid the pitfalls of the last decade that even now continue to plague Microsoft.

But don't think for a second that Macs are invulnerable or immune to security issues. Just last week I saw engineers at security software maker [Immunity](#) (in a Web-based demonstration) exploit an up-to-date version of OS X 10.6 Snow Leopard via Safari using a new, unpatched, WebKit vulnerability. All it took was clicking on a single link to give the attacker full control over the Mac.

Microsoft Rises to the Security Challenge – At the beginning of the century (all of 10 years ago) Microsoft faced one of the greatest challenges in its history. Internet worms and viruses were so rampant on the platform that it was nearly impossible to protect (or use) the systems. Unlike today's financially motivated malware, the dark side of software at the time was just as likely to erase your hard drive as steal your credit card. Microsoft then, as today, was the dominant platform among consumers, but held near-total control of the enterprise (business and government) market.

In 2001, enterprise IT professionals sweated as the Code Red and Nimda worms, and viruses like Melissa and LOVELETTER, wreaked havoc with their systems. Firewall and antivirus companies rejoiced in the massive increases in sales, but few others enjoyed the new reality.

The situation was so out of hand that Microsoft's largest customers confronted the software company and stated, in no uncertain terms, that Windows was so difficult and expensive to secure that they faced no other option but to absorb the extreme costs and move to another platform. Microsoft responded in 2002 with the Trustworthy Computing Initiative: a massive realignment of corporate priorities in which security would take precedence over time-to-market and other factors. One of the cornerstones of this program was the creation of Microsoft's Security Development Lifecycle (SDLC), a process for integrating security into every phase of software development.

Continued on page 8

Apple's Security Past Defines Its Future

Although it's still commonly believed that Microsoft software is insecure, the reality is the company is now a leader in developing secure software and responding to security issues. What most fail to acknowledge is that the large majority of serious security problems affecting Microsoft involve older products, especially Windows XP. These products never went through the cradle-to-grave SDLC, and instead still rely on a series of fixes and patches. Problems are exacerbated by serious weaknesses in third-party software like Adobe Flash (now entering its own SDLC program) and Java.

The first Microsoft product released after undergoing the complete SDLC process, SQL Server, suffers fewer software vulnerabilities than any competing database platform (a mere handful over a matter of years). Windows Vista was the first consumer operating system to undergo the SDLC and is materially more secure than Windows XP (albeit nearly unusable from a user interface standpoint). More recently, Windows 7 has blended usability, performance, and security into a fairly solid platform that is much more difficult to exploit.

But Windows XP is still the dominant Windows version in the hands of users, even though it's no longer available from Microsoft, and it's impossible to experience the benefits of Microsoft's recent security initiatives without upgrading to a modern operating system.

Apple's Unix Roots and Market Share — The same year Bill Gates announced the Trustworthy Computing Initiative, Steve Jobs released OS X. Based on a Unix foundation, OS X was, at the time, more secure than Windows XP due to how it handled user accounts. Most Windows users needed to run their systems as administrators, while OS X users ran at a lower privilege level, but could enter their passwords when they needed to perform something requiring greater rights, such as installing software. Although merely a speed bump to attackers, the feature did offer a little more security.

Coming off the corporate difficulties of the 1990s, Apple's market share was in the single digits, with comparatively few users outside the education and media markets. In the late 1990s and early part of the 21st century, Microsoft software was both easier to exploit, and ridiculously dominant.

The Mac's low market share also inadvertently conveyed additional security benefits. Those miscreants learning to write viruses and other malware were far less likely to use Macs themselves. Windows PCs were cheap, easily available, and a more common platform for teaching programming. The bad guys weren't using Macs, Macs were somewhat more secure, and there were far more Windows targets in the world.

More Macs, But a Different Environment — Any glance around a coffee shop or peek in an Apple Store tells us Macs are more popular than they've been in decades. Some Mac defenders like to point out that despite this increase in market share, there has been very little increase in security problems, and claim that this must mean Macs are inherently more secure. On the other side are naysayers who are convinced that any day now Macs will face the exact same security challenges as Windows users.

Both sides fail to realize that users of current Windows versions don't face nearly the problems of those on Windows XP, and that Macs now exist in a completely different environment than ten years ago.

Windows 7 faces a fraction of the malware that successfully attacks previous versions. Many of the attacks that do work rely on Adobe Flash or Reader, or on Java (and, as mentioned earlier, Adobe is finally focusing on security improvements).

Apple has also had time to learn and improve their own security. Snow Leopard includes many of the same security controls used in Windows 7. The one big exception is an incomplete implementation of Library Randomization (called ASLR on Windows). But, as [demonstrated by security researcher Stefan Esser](#), there's no technical obstacle to fully implementing Library Randomization on OS X. Combined with other security technologies like Data Execution Protection and a 64-bit operating system, these features significantly improve the security of any operating system.

Apple also seems to be taking the enterprise market more seriously. Apple approaches enterprises from exactly the opposite direction that Microsoft does. Rather than focusing on the enterprise first, Apple concentrates on the consumer, then slowly lowers any barriers to enterprise adoption (such as continuously increasing support for Microsoft Exchange, corporate VPNs, and enterprise provisioning of mobile devices). Apple knows that if security issues become endemic to their products, the odds of continuing their enterprise success rapidly drop off a cliff.

And finally, the malware ecosystem simply isn't in place for OS X. Few malware writers start from scratch; they use common toolkits and packages to create custom variants of, or add "features" to, existing code. This doesn't prevent anyone from attacking Macs, but it does mean greater effort is involved. There's no reason to chase a gazelle if a flock of sheep is sitting in front of it.

Mac users will never face the same environment that Windows users did a decade ago when malware became such a persistent issue. The only fair comparison is against Windows 7 users today, who also live in a far more secure world.

Positive Signs in iOS and MobileMe — Apple's most popular platform, iOS devices, faces a different situation. Apple has near-total control over the devices, including the entire application ecosystem. While iOS devices are far from perfectly secure (every jailbreak is a successful security

exploit), the very tools Apple uses to maintain platform control also enhance user security.

iOS devices use a combination of hardware and software security to protect the platform. Although we've seen security issues, there is yet to be any significant exploitation of non-jailbroken iOS devices. The single most popular smartphone in the world for the past couple of years has yet to experience a widespread security issue. Why? Because hardened platforms take more effort to develop malware for.

MobileMe is another example of Apple taking security more seriously. All MobileMe communications are now encrypted by default, something still not supported by other major webmail providers except Google. Apple improved MobileMe's security before it experienced significant problems.

Apple's Security Future — Apple still suffers from many of the security issues I identified in [“Five Ways Apple Can Improve Mac and iPhone Security”](#) (3 June 2009). The exploit demonstration I mentioned at the beginning of this article was performed using a known WebKit vulnerability that has yet to have a patch available. Apple still hasn't completed Library Randomization, and some vulnerabilities in recent patch sets appear to be signs of weak security development and testing.

While Apple still hasn't resolved some of these fundamental issues, for the most part users remain unaffected. It's easy to criticize Apple's lagging responses, but until problems affect users on a large enough scale to affect sales, it's hard to argue with Apple's actions. The one case of wide exploitation I'm aware of was related to a DNS issue on OS X servers—the Apple platform that tends to be at the bottom of the priority heap.

But OS X contains all the core pieces for a very secure operating system, and if there's one thing Apple proves time and again, it's that they are extremely sensitive to anything that will hurt their growing success. It's unlikely the well-known security experts Apple has hired of late would take such positions if they didn't think they could have an effect on the company and its products.

Possibly even more significant is the rise of the iOS and Mac App Stores. Providing users a centralized, controlled source for applications reduces the chance they will download random garbage from the dark corners of the Internet. Sure, some people will still take risks in order to find naked pictures or to lose their savings in rigged gambling halls, but most users will likely stick to the safer shopping mall.

Apple users will surely suffer greater security challenges as the use of Macs and iOS devices grows. But attackers don't have nearly the open playing field they did for a decade or so on Windows. Macs will never be as completely exposed as previous versions of Windows, and it is inconceivable that Apple wouldn't respond rapidly to anything threatening consumer perceptions and product sales.

The biggest threat to Apple users isn't any particular vulnerability or weakened security feature, but the slow decline of Windows XP. The real issue isn't Mac versus Windows, but OS X and Windows 7 versus Windows XP. Once attackers face two hardened platforms, instead of two hardened platforms and a diamond-filled defenseless baby slug, that's when market share starts to really matter.

In practical terms this means our security problems will likely exist as a series of isolated events and user-focused trickery rather than as a Windows XP-like pandemic. Apple will surely continue to tighten the security screws, and, based on their staffing trend, they are far more likely to respond quickly to serious issues today than even a few years ago. 🗑️

by Tim Sullivan

March Software Review

WavePad 4.53

<http://www.nch.com.au/wavepad/index.html>

Requires OS X 10.2 and above. \$76.

I've been looking for a sound editor that works on MP3 and Apple's AAC files. This is it.

WavePad is a sound editor program for OS X. This software lets you make and edit voice and other audio recordings. You can cut, copy and paste parts of recording and, if required, add effects like echo, amplification and noise reduction. Features: Sound editing functions include cut, copy, paste, delete, insert, silence, autotrim and more.

Audio effects include, amplify, normalize, equaliser, envelope, reverb, echo, reverse, sample rate conversion. Special effects include reduce vocals, distortion, chorus and more.

Once you open a file or begin recording via your sound card, you'll see a large rendering of the waveform, and you can choose to apply edits to the entire track or only certain parts. The application lets you open several files at once and move sound fragments among them, and the inclusion of a batch-conversion utility is a nice touch. WavePad offers a decent number of basic effects, such as noise reduction,

Continued on page 10

March Software Review

normalizing, fading, amplification, echo, changing speed and pitch, and reverb, and you can preview any edits before saving. There are also text-to-speech and speech recognition functions.

Audio Editor Features

- Sound editing functions include cut, copy, paste, delete, insert, silence, autotrim and more
- Audio effects include, amplify, normalize, equaliser, envelope, reverb, echo, reverse and many more
- Includes free sound effect and music library
- Supports almost all audio and music file formats including mp3, wav, vox, gsm, wma, au, aif, flac, real audio, ogg, aac, m4a, mid, amr and many more
- Batch processing allows you to apply effects and/or convert thousands of files as a single function
- Tools include spectral analysis (FFT), speech synthesis (text-to-speech) and voice changer
- Audio restoration features including noise reduction and click pop removal
- Supports sample rates from 6 to 196kHz, stereo or mono, 8, 16, 24 or 32 bits
- Works directly with MixPad multi-track audio mixing and Express Burn CD Recorder.
- Easy to use interface will have you editing in minutes

Apple Updates

Xerox Printer Drivers 2.1 for OS X 10.6 February 23, 2011 – 32.62MB

System Requirements
– OS X 10.6

This download includes Xerox printing software that shipped with OS X 10.6 (Snow Leopard).

HP Printer Drivers .2.6 for OS X 10.6 February 23, 2011 – 451.38 MB

System Requirements
– OS X 10.6.1 or later

This download includes the latest HP printing and scanning software for Snow Leopard.

Epson Printer Drivers 2.6 for OS X 10.6 February 23, 2011 – 845.67 MB

System Requirements
– OS X 10.6 or later

This update installs the latest software for your Epson printer or scanner.

Digital Camera RAW Compatibility Update 3.6 February 16, 2011 – 6.45 MB

System Requirements
– OS X 10.5.8
– OS X 10.6.5 or later

This update adds RAW image compatibility for the following cameras to Aperture 3 and iPhoto '11:

- Canon EOS Rebel T3 / 1100D / Kiss X50
- Canon EOS Rebel T3i / 600D / Kiss X5
- Olympus E-5
- Panasonic Lumix DMC-FZ100
- Pentax K-r
- Pentax K-5

It also addresses processing issues for the following cameras:

- Nikon D7000
- Nikon COOLPIX P7000
- Panasonic Lumix DMC-GF1
- Panasonic Lumix DMC-GH2

iWeb 3.0.3 February 15, 2011 – 177.12 MB

System Requirements
– OS X 10.5.8
– OS X 10.6.3

This update contains bug fixes and improvements, including the following:

- Addresses an issue when using the iSight Movie widget on certain Macs
- Addresses an issue publishing iWeb sites using FTP
- Improves compatibility with OS X

Lexmark Printer Drivers 2.4 for OS X 10.6 February 02, 2011 – 139 MB

System Requirements
– OS X 10.6 or later

The Lexmark Printer Driver Update includes the latest drivers for printers you have used on your system. 



Mac 911

Creating custom GarageBand samples

Reader Skip Edwards seeks an additional way to tinkle in GarageBand. He writes:

I have a little toy piano that I would like to sample and use in GarageBand, but I have no idea where to start and what software to use. Is there a (simple and cheap) way to sample this instrument and then use it as a software instrument sound in GarageBand?

Yes. This can be done for free if you have a microphone that works with your Mac.

You'd use that microphone in league with a recording application such as the free and open-source Audacity to record each note of your toy piano. I don't want to turn this into a tutorial on how to record audio, so here's the gist. Create a new file, place your microphone in a position where it can capture the best your piano has to offer, start recording, and plunk out a note on the instrument, letting it ring for as long as it sounds natural (which, for a toy piano, shouldn't be too long). Name the sample (TP C3, for example) and save the file in the AIFF or WAV format. Create a new file for each note you eventually want to play in GarageBand.

Launch GarageBand and choose a new Piano project. In the resulting window, select the Grand Piano track and press Command-I to produce the Info pane. In the first Browse column select Sound Effects. In the Instrument column to the right, select Radio Sounds. Now choose Window —> Musical Typing. Locate the samples you recorded of your toy piano and drag them into position on the Musical Typing keyboard — for example, drag the Middle C sample to the correct position on the Musical Typing keyboard. If you have more samples than will fit on the keyboard, choose a lower or higher octave from the keyboard at the top of the window and drag in your samples.

GarageBand's Musical Typing keyboard Once you've loaded all your samples, click the Save Instrument button at the bottom of the window. You'll be prompted for a name for your instrument. Enter it and click Save. That instrument will now appear in the Instrument column when you select Sound Effects in the Info pane. Like other software instruments it can be played with both GarageBand's virtual keyboard and an external musical keyboard.

If you'd like more control over your samples, check our SonicAmigo's \$35 PolyPhonics GB. With it you can tweak your samples to a far greater extent.

Picture-in-picture iChat presentations

Reader Soren Peterson is seeking a more personalized presentation. He writes:

I'm scheduled to do a presentation with people thousands of miles away. They're Mac users so I was hoping that I could use iChat. I'd like to show them a Keynote presentation but I'd also like them to be able to see me via my MacBook's iSight camera. Is there a way to do that?

There is. Just follow these steps:

1. Launch iChat, locate the person you'd like to chat with in the Buddy list, and click on the Video icon next to their name.
2. After they've accepted your video chat invitation and you can see each other choose File -> Share a File With iChat Theater.
3. In the Share With iChat Theater window that appears, navigate to your Keynote presentation and click the Share button.

Your iChat window will now display the first slide of your Keynote presentation. In the bottom left corner you'll see the image from your buddy's camera. On their end, they'll see a similar arrangement but your camera's image will appear in their window.

4. Another window should also appear on your Mac — one called Playing Slideshow: nameofpresentation. This window belongs to Keynote. In it you'll find navigation controls for your presentation — Previous, Next, Full Screen, and Close. Use these controls as you would with any Keynote presentation. (You can also use the Space Bar and Arrow keys to navigate your presentation.)

When you're finished with your presentation just click the Close button and your iChat window will return to its usual picture-in-picture view.

Projecting the iPad's entire interface

Last week during Macworld 2011 (formerly known as Macworld Expo) I spent a portion of my time standing in front of attendees demonstrating one thing or another on an iPad. Unlike other presentations that similarly projected images from an iPad, the images from my iPad were darned near pristine. This is the story of how I did it.

Continued on page 12

Mac 911

First, the backstory: In years past, when Ben Long and I have presented our iPhone Supersession, we used an Elmo projector system. This is essentially a camera that points down at a white base. You place the object you want to show on the base and its image is transmitted to a projector. Because only Apple had the secret for projecting an iPhone's entire interface, mere mortals had to depend on the camera-to-projector solution, which is less than ideal because the image can be fuzzy.

This year, when planning our new iPad Supersession, I thought it would be worth exploring alternatives to the Elmo. If there was a way to hack the iPad so that it displayed the iPad's entire interface (as this was something we intended to show to our audience) via a standard projector connection rather than Elmo, we'd be ahead of the game. I discovered that alternative in the form of a jailbroken iPad. Specifically, with the help of a tethered jailbreak, Apple's \$29 iPad Dock Connector to VGA Adapter, and Ryan Petrich's \$2 Display Out (available through the BigBoss Repository in Cydia), our audience enjoyed a crystal-clear view of my iPad. Here are the steps:

1. Understanding the jailbreak. There are two kinds of jailbreaks — tethered and untethered. A tethered jailbreak requires that you re-jailbreak your device every time you completely power it off or restart it. With an untethered jailbreak, the jailbreak will stick even after you've restarted the device. Obviously an untethered jailbreak is preferable, but currently the untethered jailbreak for iOS 4.2.1 is in beta. I wanted a reliable jailbreak and so chose to go with the tethered method.

2. Obtain the tools. To perform the jailbreak you need a copy of redsn0w (this is a direct download link to the tool that performs the job) and a copy of your iPad's software. You might find it by following this path: youruserfolder/Library/iTunes/iPad Software Updates. If you don't, because it's been thrown away by iTunes, you can directly download it here (another direct download link).

3. Perform the jailbreak. Plug your iPad into your Mac and power it off. Launch redsn0w by double-clicking on it. In the window that appears, click the Browse button. A Browse for IPSW window will appear. Navigate to the iPad Restore.ipsw file and click the Open button.

redsn0w will go about its business of identifying the iOS software and report "IPSW Successfully Identified." After you click the Next button, redsn0w will process and patch the iOS software.

The next window asks you to select an option. "Install Cydia" is enabled by default. Leave this as the default and click Next. A warning next appears that tells you to leave

the iPad powered off but plugged into your Mac. When you've granted these requests, click Next again.

In the following window you'll find instructions for putting your iPad into DFU (Device Firmware Update) mode. This involves holding the On/Off button for a few seconds, pressing the Home button while still holding the On/Off button, and then letting go of the On/Off button while continuing to hold the Home button. The window signals when to do all this.

redn0w will now jailbreak the iPad. But you're not done yet. You need to run redsn0w one more time. And yes, this means powering off the iPad while it's connected to your Mac.

Follow the same steps as you did before, except this time, when you get to the options screen, choose the Just Boot Tethered Right Now option and click Next. Again, you'll be asked to put the iPad into DFU mode and then redsn0w will complete the process.

When your iPad has booted you will see the Cydia app on your home screen. You'll use this app to obtain the Display Out hack that lets you project all of the iPad's interface. It's likely that Cydia will tell you that some of its components are out of date and offer you the option to update them. Do that. You will have to reboot your iPad, which means you have to run redsn0w yet again and choose the Just Boot Tethered Right Now option.

4. Obtaining Display Out. One of Cydia's many charms is its Cydia Store — a place where you can purchase apps not allowed by or submitted to Apple's App Store. The app that you want is Display Out.

To get it, launch Cydia and tap Manage Account. In the screen that appears choose either Connect With Facebook or Sign in With Google (depending on the kind of service you want to connect Cydia to). Once you enter either your Facebook username and password or Google username and password you'll be asked to allow a connection between Cydia and the service. When you tap Allow, you'll then be asked to link your iPad to this account. This is simply for verification purposes.

To obtain Display Out, tap the Search icon at the bottom of the Cydia screen and start typing Display Out. It will appear in the list of available apps. Tap it and a Details screen will appear that includes a Purchase Package option with the price next to the app. Tap Purchase Package and you'll see that you can purchase via your Amazon or PayPal account. Choose the option you like. You'll be prompted to enter the e-mail address and password for your Amazon or PayPal account. Do this and eventually you'll be allowed to download the app.


After you've downloaded and installed the app, you'll be told that you need to reboot your iPad. Rather than tap Reboot, press the Home button and then hold down the On/Off button to shut down the iPad.

Yes, this means you have to run redsn0w again. The reason I suggest you do this is because if you reboot from Cydia you'll find that the iPad will hang on the Apple logo during the startup process. The unjailbroken version of the iOS conflicts with Display Out, making it more difficult to reboot when tethered. When you shut down the iPad and reboot via redsn0w you don't have this problem.

5. Make the connection. You're finally ready to project your iPad. Simply attach Apple's iPad VGA adapter to your iPad's dock connector port, string a VGA cable between the adapter and your projector, and launch the Settings app. (Apple's Component and Composite AV cables work too, but the image isn't nearly as good as what you get with the VGA adapter.) At the bottom of the list of settings you'll see Display Out. Tap it and the Display Out settings appear to the right. In my experience I found that choosing 16:9 in the Aspect Adjust area worked best, but feel free to play with that setting to see what works for you. You can also use the Scale slider to make the image bigger or smaller to fit the screen. It's also worthwhile to switch on the Show Taps option. This places a dot on the screen that indicates where you've tapped.

Note that if you power off your iPad or restart it (not put it to sleep) with Display Out installed, there's a very good chance that the iPad will stall at the Apple logo when it attempts to boot up. In this case you'll need to tether it to your Mac and run redsn0w again — yes, even though you can't shut it completely down — and choose the Just Boot Tethered Right Now option.

Whew.... What a pain, right? Honestly, it's not as bad as it sounds although it's tiresome that you can't turn off or reboot your iPad without losing the jailbreak. In a perfect world Apple would provide the capability to display an iOS device's entire interface. Doing so would make a lot of teachers, technicians, and presenters happy. And, of course, we'll all celebrate the day when an untethered jailbreak is fully baked. Until that day, this is the way to offer more perfect iPad presentations to your audience.

*"OS X 10.5 Leopard Essential Training (video)" from lynda.com
Find Chris' books at www.amazon.com and www.peachpit.com.
Get special user group pricing on Macworld Magazine!
Subscribe today at <http://www.macworld.com/useroffer> *



Share Keystone MacCentral with other MACaholics

Name _____

Address _____

City _____ State ____ Zip _____

Home Phone _____ Day Phone _____

E-mail Address _____

Date _____ Is this Renewal or New?

How did you hear about us? _____

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

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

**Keystone MacCentral
Membership Chair
310 Somerset Drive
Shiresmanstown, PA 17011**

Keystone MacCentral meetings are **usually** held at 6:30 p.m. on the 3rd Tuesday of the month at Giant Foods, Trindle & 32nd, Camp Hill