

printout

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



Join us on December 16th
for our annual
Keystone MacCentral Holiday Party.
We will have our business meeting and Q & A period,
followed by a program that will include
plenty of time for eating and socializing.
KeyMac will provide soda and some munchies;
we ask members to bring in
something good to share.
The evening's program will include
a presentation on Mac OS 10 Yosemite:
creating a bootable installation disk
and some of the new features.

Meet us at

Bethany Village Retirement Center

Education Room

5225 Wilson Lane, Mechanicsburg, PA 17055

Tuesday, December 16, 2014 6:30 p.m.

Attendance is free and open to all interested persons.

Contents

Annual KeyMac Christmas Party	1
President's Corner by <i>Linda J Cober</i>	3
Keystone MacCentral Minutes by <i>Gary Brandt</i>	4
iCloud Drive Is Not a Dropbox Replacement by <i>Michael E. Cohen</i>	5 - 6
How to Reclaim Your Phone Number from iMessage by <i>Josh Centers</i>	7
First Apple Watch Apps Will Only Skim the Surface by <i>Michael E. Cohen</i>	7 - 8
Apple's Auto-Correct Spelling	8 - 9
You Are Apple's Greatest Security Challenge by <i>Rich Mogull</i>	9 - 12
November Software Review	12 - 14
Maps to our new meeting room	15

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 Inc. Copyright © 2014, Keystone MacCentral, 310 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

Tim Sullivan

Program Director

Gary Brandt

Membership Chair

Eric Adams

Correspondence Secretary

Sandra Cober

Newsletter Editor

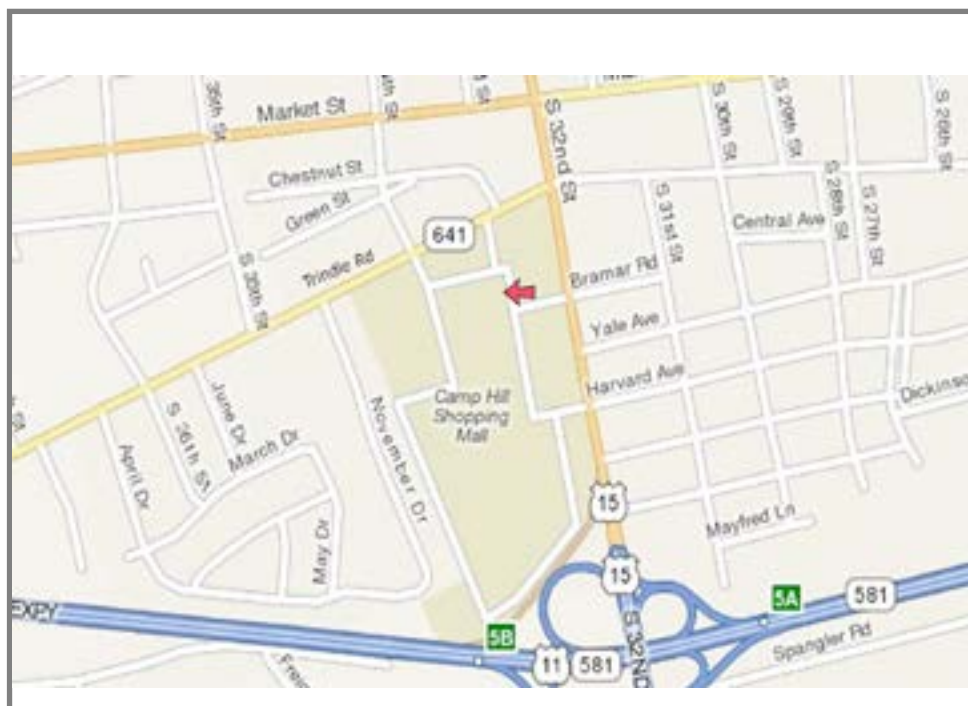
Tim Sullivan

Industry Liaison

Wendy Adams

Web Master

Tom Bank II



Keystone MacCentral Essentials

Meeting Place

Bethany Village West
Maplewood Assisted Living (Bld 21)
5225 Wilson Lane
Mechanicsburg, PA 17055

Web Site

<http://www.keystonemac.com>

Mailing Address

310 Somerset Drive
Shiresmanstown, PA 17011

President's Corner

Our December 16 meeting will be a good one, and I hope you will be there! For the first time in a number of years, we will be having our traditional Christmas party as well as an informative program. When we met at the Giant Community Room, we appreciated their hospitality but any food had to come from Giant, and that did not mean that we could buy the ingredients at Giant and bring in homemade cookies. Now that we are meeting at Bethany Village West in the Education Training Room, we can bring in our own special treats and goodies for all to share. Unfortunately, the Adams family will not be with us because of a program at school, and that means that Wendy will not be making her delicious chili for us. However, my sister Sandy and I discussed this loss and decided that our first Christmas party at Bethany should not be without chili, so instead of Adams' family chili, we will have Cober family chili. Thus, you may not want to eat dinner before you come to the KeyMac meeting, which starts as usual at 6:30, but should bring along your favorite goodies to share. Those goodies can be sweet or salty, and we hope to have a good selection for everyone to enjoy, so have fun deciding what to bring and join us for a great meeting and party!

On another note, if you have been wondering about whether to buy an iPhone 6 or an iPhone 6+, Sandy and I can show you the new iPhone 6+ since we just got our new ones at Best Buy on Black Friday. We got our phones there because Best Buy was offering a minimum of \$100 for working iPhones, and we wanted to take advantage of that offer. Sandy turned in her iPhone 4s for \$105, while I turned in my iPhone G3 and got \$100-what a deal! We both got the 64GB version because with operating systems continuing to become more complex and thus bigger, combined with our penchant for taking photos, we knew that anything smaller would be a mistake. Right now, I have over 44GB available with all my photos from my old phone on the new one, so I am feeling good. Of course, by the time we are ready to buy new iPhones, I am sure that 64 GB will seem small. Can you remember wondering why anyone would ever need a hard drive with over 60 megs of storage? Yep, time and technology move on!

Remember, our December 16 meeting is a party and meeting combined, and you are invited to bring goodies to share. There will be chili for the main course, and KeyMac will provide soft drinks, bowls, spoons, plates, napkins, and cups, so get ready to join your KeyMac friends for an evening of fun and enlightenment! Party on! 🍷



Keystone MacCentral Minutes

November 18, 2014

Business Meeting

We plan to have our annual holiday party at the December 16th KeyMac meeting. Outside food and drinks are permitted at Bethany Village and we are inviting members to bring goodies for that meeting. The club will provide sodas, ice, plates, napkins, and utensils.

Eric Adams asked members to send him names of any vendors he could contact for our next auction.

Q&A & Comments

As we were settling in for the meeting, Jim Carey showed us a slideshow of images from a recent Hershey Camera Club contest. He explained how he had created it using iPhoto. These iPhoto slideshows can be exported as movie files.

Ernie Levasseur asked how iPhoto works in Yosemite. It will work although a new Photos app is set to be released by Apple. Jim Carey strongly recommended duplicating your existing iPhoto libraries and moving the duplicates onto another hard drive before updating them to work with the new Photos app.

Eric Adams mentioned a few minor problems he had encountered with Yosemite. Jim demonstrated using Reflector to mirror an iPad or iPhone screen onto the room's projection screen for some guests who had not seen it before. Jim asked about making references between different pages on Numbers spreadsheets.

Program Notes

Jim Carey showed us how he uses FileMaker Pro Advanced to maintain membership lists. He mentioned that owners of FileMaker 12 or 13 can use FileMaker Go for free. The first step in setting up a database is having an idea of what the finished project should look like and what items are necessary for inclusion. FileMaker Pro presents the user with a menu of layout choices that can be set up in advance. Jim's sample database used for the demonstration had the standard name and address fields as well as other fields that Jim added and defined. Jim added a button that has some pre-defined selection options. One option lets

him select a group of members whose membership has lapsed within the last month or two. Pop-up lists for frequently used entries can be created and calculations can be set up. The program is capable of sending out emails using a POP email account. Some daily limits might be set up by your email provider. For example, a daily limit of 100 emails is imposed when using gmail. Eric Adams mentioned that dropping a Excel spreadsheet file onto FileMaker Pro creates a new database file populated with field data from the spreadsheet. Some editing will be required but this method may save you a lot of time.

If you want to work with your database file with FileMaker Go on your iPad or iPhone, you can email yourself a copy of the file from your Mac. Jim did this with his sample database which he then opened on his iPad. Records can be added or edited and then saved and emailed back to the Mac. If you have an Airprint capable printer, you can print directly from FileMaker Go.

Jim navigated to his [Kelby Training](#) account to show us their offerings. Their focus is on using Adobe products for photography projects. [Lynda.com](#) is a good place for training on apps and operating systems. Kelby and Lynda.com offer one month trials so users have a chance to see if they want to register for longer periods.

Eric Adams demonstrated [Udemy](#) and its multitude of course offerings. Free previews of many of the courses are available. Eric also displayed a phishing email he had received asking him to validate his Apple ID. He knew it was not legitimate because it referred to a device he did not have. Beware of these phishing attempts. If something does not look quite right, it is best not to reply to any links in that email. ☹



iCloud Drive Is Not a Dropbox Replacement

After I wrote “[Moving to iCloud Drive](#)” (15 October 2014), I received several messages asking me how to use iCloud Drive as a Dropbox replacement. As I said in several responses to those inquiries, “iCloud Drive is not a replacement for Dropbox.” But I don’t blame the inquirers for the confusion: Apple has not done a stellar job explaining iCloud Drive, nor, for that matter, iCloud in general.

Part of the problem is that iCloud is not just one thing but a whole panoply of services, including calendar and contact storage and syncing, email, location services, media and app sharing, backup, data storage, document storage, and more. From time to time, Apple highlights one or more of these services in its marketing, usually when it is introduced or expanded, but to my knowledge the company has never provided a comprehensive guide to the entire beast. That’s one reason Joe Kissell’s “[Take Control of iCloud](#)” has been so successful (and yes, he’s working hard on an update that will be out shortly). As a result, we end up like [the blind men in the story about the elephant](#), each of us thinking that iCloud is whatever part of the elephant that we have happened to have laid our hands upon.

iCloud Drive is one part of the iCloud elephant, but Apple has not gone to great lengths to explain which part of the beast it is, so it’s easy to think that iCloud Drive is a brand new animal. But it’s neither completely new nor its own animal. It’s simply a more mature form of an existing iCloud feature: Documents & Data.

Documents & Data – Before Apple introduced iCloud Drive, each iCloud-compatible app could have its own private storage space in a user’s iCloud account. Only that app could access that space and manipulate the files stored in it. Apple slapped the generic name “Documents & Data” on that capability when talking about it to users and exposing it in interfaces. Here’s how it worked.

If an iCloud-enabled iOS app (like, say, Pages or PDFpen) had a related Mac app that also used iCloud, the Mac app and the iOS app could both access the same private storage space and use the same files. This meant that you could create a file on your iPhone, save it in iCloud, and open it on your Mac or your iPad in the related app.

However, even on the Mac, you had to use the app to create, delete, or modify files in its private iCloud storage space; the Finder had no direct access to it. (Technically, you could delve deep inside your Home folder’s Library with the Finder and find the cached iCloud files, but those cached files inside your Mac’s Library were only local

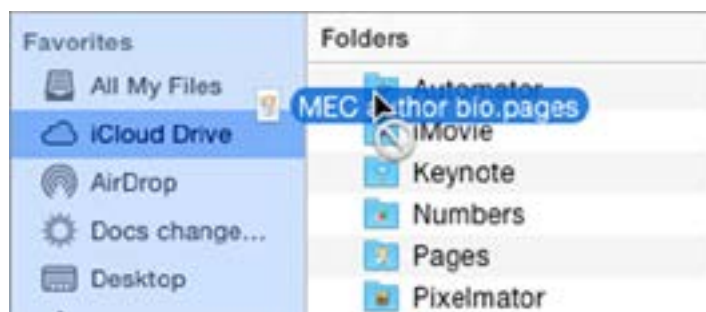
copies and not guaranteed to reflect the current “truth” — that is, the master file as it was stored in iCloud itself.)

With OS X 10.10 Yosemite and iOS 8, Apple introduced iCloud Drive. But it wasn’t a replacement for Documents & Data. What it did was provide a user interface for the Documents part of Documents & Data.

iCloud Drive – On the Mac, iCloud Drive provides a Finder-accessible method for viewing, adding, and removing the documents that apps store in iCloud. In addition, it gives users a way to create their own folders in iCloud and put whatever documents they like in those folders. iCloud Drive appears as a choice in the Favorites sidebar of Finder windows and, when clicked, displays what looks very much like a normal list of folders. Looks, however, can deceive.



Many of the folders shown in iCloud Drive — in fact, all of them if you haven’t added any of your own — are not Finder-type folders at all but “app libraries.” These app libraries are how the formerly private document storage spaces for apps appear in iCloud Drive. They are still managed and maintained by the apps that own them, and what you can do with them is still largely dictated by individual apps. For example, some apps may restrict the kinds of documents you can put into their app libraries. You can’t even Get Info on an app library “folder” in the Finder; File > Get Info is disabled, and if you try the Command-I shortcut, the Finder beeps at you.



In iOS 8, which has no Finder, iCloud Drive can be accessed from within iCloud-enabled apps — if, of course, the app's developers provide that capability. In most cases, iCloud-enabled apps in iOS 8 display the iCloud documents they manage in much the same way that they did in earlier versions of iOS.



However, even when they display their documents in the same old way, apps can also provide a method for browsing iCloud Drive and opening compatible documents stored in other app libraries or user folders. For example, in Pages for iOS, tapping the + icon on the document manager toolbar can take you to the iCloud Drive “document picker,” from which you can open user folders and other apps’ libraries (for those apps that allow you; some libraries may be disabled or not even appear in the picker), and, from within those libraries or folders, choose documents to open.



It's hard to predict what an app will do when you open a document from another app's app library or from an iCloud Drive folder. One app may make a copy and store it in its own app library; another may create an alias and store that in its app library.

For the most part, iCloud Drive simply gives you more control and convenience for managing the Documents

part of the old Documents & Data service than previous versions of iOS and OS X offered. However, because it also allows you to make your own folders on iCloud Drive — even within some app libraries — and to store whatever documents you want in your folders, you can't be blamed for thinking, “This here sure looks like I could replace Dropbox with it!” You would most likely be wrong, though.

iCloud Drive Isn't a Dropbox Replacement — To begin with, Dropbox is far cheaper than iCloud: \$99 per year for one terabyte of storage for Dropbox versus \$19.99 per month (or \$239.88 per year) for the same amount of iCloud storage.

But cost is just part of the reason: the two services also work differently. Take sharing, for instance. iCloud is generally all about sharing, but it's mostly about sharing your stuff with your devices: that is, sharing the same stuff (calendars, music, mail, your budget in Numbers, and your half-finished novel in Pages) among all of your devices. Sharing stuff with other people, even other iCloud users, is not easy, and worse, the options are limited and tightly focused (such as specific photo streams or explicitly shared documents in Pages or Numbers).

Dropbox, on the other hand, lets you share folders and all the documents therein with other Dropbox users — this is how Take Control manuscripts are made available to authors and editors for writing, editing, and production. Doing the same thing with iCloud Drive would be impossible.

Furthermore, iCloud, unlike Dropbox, doesn't store previous versions of a file (though some individual apps do), nor does it let you restore deleted files.

Most importantly, though, iCloud Drive is not just a file sharing service. Remember that apps on both Mac and iOS have a lot to say about what you can do with their app libraries. This means that the Finder, in order to create the illusion that iCloud Drive is just another drive with a bunch of folders and yet respect those individual apps' rights and requirements concerning their own stuff, can behave unpredictably. You can't tell by sight, for example, which app libraries will accept which files until you try them.

Also, at least in the initial release of Yosemite, the Finder can get confused when you do some seemingly normal file handling things within the confines of an app library, such as changing the name of an alias created by an iOS app. I have seen the Finder go into a spinning beachball mode from which it doesn't recover when I have done that; other times I have seen the changed filename turn into a long string of letters and numbers. This is not the sort of behavior you want in a file sharing service.

For what it is — a better way to manage, access, and sync your documents stored in iCloud — iCloud Drive is a welcome enhancement.

But it isn't Dropbox. 🗑️

How to Reclaim Your Phone Number from iMessage

When it works, iMessage is one of Apple's best online services. With iOS 8 and OS X 10.10 Yosemite, it seamlessly merges SMS and instant messaging across all your Apple devices, and you won't find better security in a mainstream messaging app. (No, really! See "[EFF: Apple Offers Best Mainstream Messaging Security](#)," 7 November 2014.)

But if you decide to switch away from the iPhone to any other type of mobile phone that uses SMS text messages instead, iMessage can become a Kafka-esque nightmare. That's because messages sent to your phone number from your Apple device—using "blue bubble" friends would still go through iMessage and into the void, unless you had disabled iMessage in Settings > Messages on your iPhone. Previously, if you forgot to disable iMessage before getting rid of your iPhone, you were in for long phone calls to Apple to remedy the situation.

Apple has finally released an [online tool](#) to disengage your phone number from iMessage (a [class action lawsuit](#) might have encouraged its creation). Visit the page, enter your

phone number to receive a confirmation code, and then enter that code on the site.



While it's good that Apple has released a tool to deregister a phone number from iMessage, it's infuriating that it took so long. Granted, Apple doesn't have much incentive to help customers switch to a competing platform, but to paraphrase a [common saying](#), "If you want a loyal customer, let them go. If you truly make the best product, they will return." 🗑️

by Michael E. Cohen

First Apple Watch Apps Will Only Skim the Surface

Apple released the first beta of its iOS 8.2 software development kit (SDK) to registered Apple developers last week, and it includes the initial release of [WatchKit](#), the SDK component that developers will use to make Apple Watch apps. A quick look at its contents makes clear that the first generation of third-party apps for Apple Watch will be remote display and input extensions to iPhone apps. There's nothing wrong with that, of course, but if you were hoping to see a flurry of rich, immersive Apple Watch apps pouring into the App Store from developers early next year, it's time to reset your expectations.

The WatchKit framework, the part of the SDK that provides the software interfaces that developers use for building Apple Watch apps, consists of little more than a list of the user interface objects that appear on the watch: menus, buttons, sliders, labels, tables, and the like. Missing are

interfaces for, say, playing sounds or displaying videos, or for accessing the watch's hardware features.

As the Apple Watch Human Interface Guidelines (included in the SDK) make abundantly clear, Apple Watch apps are lightweight, intended to complement iOS apps rather than replace them. The model looks something like this: an iOS app uses a WatchKit-enabled extension running in the background on an iOS device to exchange data with a paired Apple Watch in order to display information and elicit simple input from the watch's wearer. For example, a restaurant guide running on an iPhone could send listings for nearby restaurants to the watch, and the user could page through them to pick where to eat. However, given the Apple Watch's limited screen space (a paltry 340 by 272 pixels on the 38 mm Apple Watch screen, and a slightly more expansive 390 by 312 pixels on the 42 mm model), such information would have to be pared down to a bare

minimum — roughly about the same amount of content than you could send in a single tweet on Twitter.

Apple describes two basic types of user interaction with Apple Watch, and both are seen as being brief interactions, lasting just a few seconds, not complex engagements taking minutes: Glances and Notifications. Both of these types are displayed only when the watch wearer lifts the watch to look at it.

A Glance fits on a single screen and displays information from an iOS app. If the wearer taps the screen, the action opens the app on the linked iOS device that sent the information. More than one iOS app can be running at a time, periodically sending information to the watch, and wearers can swipe up to scan through the current set of Glances.

A Notification alerts the wearer via the **Taptic Engine** interface provided by Apple Watch — that is, you feel a tapping on your wrist. When the wearer raises the watch, the “short look” version of the notification appears, displaying just its bare essentials (for example, that a meeting is about to begin). A tap on the notification, or keeping

the wrist raised, reveals its “long look” which can contain more information (for example, the meeting is about to begin in 7 minutes in conference room C) as well as up to four buttons for responding to the notification. Long look notifications must be dismissed explicitly by the wearer.

WatchKit also provides Modal Sheets, much like modal dialogs on a Mac or iOS device. These take over the Apple Watch interface until the user dismisses them and are used for short tasks that require one or more steps. Modal Sheets have a close button to close or cancel the sheet.

And that’s pretty much the range of interactions that a third-party Apple Watch app can offer. At least for now. In its [press release](#), Apple did say that “Starting later next year, developers will be able to create fully native apps for Apple Watch.” So we can expect more fully featured third-party Apple Watch apps to start appearing eventually. Just not now.

And that’s OK. It’s better that Apple takes things slowly, as the company did with the original iPhone, rather than committing to decisions that might be regretted later. 🍷

Apple’s Auto-Correct Spelling

I just found the answer to the problem that has been driving me (and a lot of other people) crazy with Apple’s Auto-Correct Spelling feature. Note that nowhere I have looked in the official Apple Support web pages is there any mention of a permanent fix. Also, note that Mavericks changed the place to look for this global option from the Language & Text preferences pane to the Keyboard pref pane.

I can’t understand why, with all the complaints and frustration expressed by so many individuals, Apple doesn’t make the answer to the problem more readily available. The only reason I can think of is that they want everyone to work the same way as iPhone users do. My thought is just the opposite: If your mother wants a pad, my recommendation would be a Kindle!

Tom Bank, Sr.

One complaint I have run into with OS X Lion and later is its new auto-correct spelling feature. OS X already had a spell checker that can check your spelling as you type, but the new version of the spell checker can be a royal pain in the dictionary. The new auto-correct function is very aggressive about wanting to make changes to spelling; it also makes changes so quickly that you may not notice that a word you typed has been changed.

Fortunately, OS X Lion (and any later version of OS X) also includes a system that provides a good degree of control over the spell checker. It gives you the choice to not only enable the spell checker on a system-wide basis, but also to turn it on or off for individual applications.

To Enable or Disable Automatic Spelling Correction System-Wide

- Launch System Preferences, either by clicking the System Preferences icon in the Dock, or by selecting System Preferences from the Apple menu.
- Click the Language & Text preference pane.
- In the Language & Text preference pane or the Keyboard preference pane (OS X Mavericks or later), select the Text tab.
- To enable the automatic spelling check, place a check mark next to the Correct Spelling Automatically item.
- To disable the automatic spelling check, remove the check mark next to the Correct Spelling Automatically item.

Enable or Disable Automatic Spelling Correction by Application

Apple also embedded the ability to control spell-checking functions on an application-by-application basis. This per-application system will work with software that has been updated to work with Lion or later. Older applications may not have the ability to turn spell checking on or off, or they may have their own built-in spell-checking system that supersedes the one built into OS X.

Depending on the application, the ability and options available to control spell checking will vary. In this example, I'm going to turn off the auto-correct feature in Apple Mail. I'll let the spell-checker retain the ability to point out an error as I type, but not to auto-correct it.

- Launch Apple Mail.
- Open a new message window. The text insertion point needs to be in an editable area of the message, so click in the body of the message.
- Click Mail's Edit menu and let your cursor hover over the Spelling and Grammar item (but don't click). This will reveal a sub-menu with various options.

- Options that are enabled will have check marks next to them. Selecting an item from the menu will toggle the check mark on or off, depending on its current state.
- To turn off auto-correction, remove the check mark next to Correct Spelling Automatically.
- To allow the spelling checker to warn you of errors, enable a check mark next to Check Spelling, While Typing.
- The menu entries in other applications may look slightly different, but if the application supports the system-wide Spelling and Grammar system, you will always find options to control the various functions in the application's Edit menu, under the Spelling and Grammar item.

One last note: Setting application-level Spelling and Grammar options may not take effect until you restart the application. 🔄

by Rich Mogull

You Are Apple's Greatest Security Challenge

Apple's focus on the security of its operating systems used to be pretty minimal. Fortunately, it didn't really matter.

Spend enough time in the security world and you realize that it's defined by economics and human behavior, not technology. When I first started writing about Apple in 2006, the company had a good security team, but didn't give it many resources. It's hard to justify spending a lot on security when you aren't suffering security losses.

Just ask Microsoft. For years the company didn't invest much in security, even as Windows came to dominate the computer industry. Then the bad guys showed up, and in 2001 it became nearly impossible to protect Windows-based PCs from attack. Microsoft's biggest customers, like big banks and the U.S. government, threatened to move to something — anything! — else as the costs to install security defenses and account for security breaches skyrocketed. The result was the [Trustworthy Computing Initiative](#) in 2002. Microsoft now has the strongest security program in the industry.

In a series of what look like near-prescient moves, Apple dodged that bullet while coming to dominate the handheld device market and increasing its share of the personal computer market. Apple learned the right lessons from Microsoft's early failures, and as a result, we haven't seen any significant iOS malware (most of what there is targets jailbroken devices) or a major Mac malware epidemic. In essence, particularly with iOS, Apple put security in place early, before criminals could build an attack ecosystem.

But the future is in the cloud. And Apple's future is iCloud, the online glue that holds its entire ecosystem of devices, software, and services together. I spend most of my working hours on cloud security, and it is an indescribably difficult problem that's only getting worse as our use of these services grows. Apple, like all major cloud providers, now faces the same security issues as banks (cue the Willie Sutton reference about "[that's where the money is](#)").

Talk to any bank about security, and they'll all point to the customer account as the problem.

Chum in the Water — Little grabs attention like the words "celebrity nudes." The phrase "chum in the water" doesn't even begin to describe the resulting media feeding frenzy. Add in the world's most popular technology brand, schedule it for a few weeks before the company's biggest product announcement in years, which also included a major new financial service, and you end up with a special sort of PR nightmare.

You know the story by now. A string of nude photos of about one hundred celebrities hit the Internet over Labor Day weekend. Speculation quickly focused on iCloud backups or photos as the source, given that it came only a few days after the release of a new tool that attacked iCloud directly via a brute-force technique that most cloud services restrict (and that Apple quickly blocked).

The truth was slightly less dramatic, but no less disturbing. Within 48 hours [Apple announced](#) that iCloud in general hadn't been hacked, and the brute-force tool wasn't the vector. Instead, individual celebrities were deliberately targeted and their photos stolen, most likely via iOS backups to

iCloud. The crimes likely occurred over a long period, and the photos didn't necessarily all come from iCloud.

After more than 40 hours of investigation, we have discovered that certain celebrity accounts were compromised by a very targeted attack on user names, passwords and security questions, a practice that has become all too common on the Internet. None of the cases we have investigated has resulted from any breach in any of Apple's systems including iCloud® or Find my iPhone. We are continuing to work with law enforcement to help identify the criminals involved.

To protect against this type of attack, we advise all users to always use a strong password and enable two-step verification.

iCloud wasn't hacked, but it was. Instead of compromising some core vulnerability in the service, the criminals targeted famous users and performed a series of account takeovers. They figured out passwords or password recovery questions. I suspect they then pulled in the victims' friends and colleagues using phishing techniques based on the initial information taken. They harvested iCloud credentials, and used hacking tools to pull down copies of iCloud backups, circumventing Apple's normal new-device notifications (primarily used with Messages and FaceTime) and even two-factor authentication, which protected only purchases and core Apple ID changes.

Apple was in a bind. This wasn't an issue specific to iCloud, and the company essentially blamed its customers for not protecting their accounts well enough. And Apple then recommended a solution, two-factor authentication, that wouldn't have stopped the attacks at the time (it didn't then apply to iCloud logins or backups). Ouch.

To be fair, Apple was correct that account takeovers are an all-too-common problem on the Internet. But decisions by Apple, such as limiting the services protected by two-factor authentication, relying on password recovery questions (which are notoriously easy to circumvent, especially for public figures), and not detecting the unusual activity on the server side all conspired to make the attackers' jobs easier.

iCloud wasn't compromised in general, but that's not to say that Apple did all it could have. And even if the company had done more, there's no guarantee that such persistent attacks could have been prevented. Account takeovers are incredibly serious, impossible to eliminate, and likely the single greatest challenge as we continue to expand our reliance on cloud computing.

Where Password Equals "Gordian" – Proving identity is a complex problem, especially since the concept of identity itself is somewhat ephemeral. Just ask any friend with a common name, like our own Michael Cohen ([who is not any of these people](#)). In the digital world, we worry less about proving identity and more about authentication, which is proving to the computer that you are the person associated with a specific account.

We do this using something you know (a password), something you have (a digital token like a smart card or a code from an iPhone app), or something you are (a fingerprint). The more of these things that are checked, the stronger the authentication.

Passwords are nearly always used as one of the authentication factors. Tokens cost money and are easy to lose. Fingerprints, or any biometric factor, raise serious privacy issues and are hard to work with reliably. Neither tokens nor fingerprints are well suited for logging into remote services, since everyone would need their own readers. Imagine having to swipe your credit card to log in to every Web site. The complexity of these systems, at scale, is nearly insurmountable with current technological and social limitations. Who provides the cards? Who manages your fingerprint template? How is this all communicated? In many cases tokens and fingerprints are less secure than passwords which is why we tend to use them as a second factor, not the primary one.

Reducing our reliance on passwords may not be an impossible problem, but it's one we're a long way from solving.

Compounding the problem is the issue of account ownership and recovery. We forget passwords. We lose smart cards. Our fingerprints change. We can't let those facts restrict access to our accounts, so we add recovery mechanisms. It might be another, stronger, password we tell the user to write down and store safely — but anything written down isn't safe by definition. Or perhaps we require security questions we hope only the account owner can answer, but to be memorable, they have to be discoverable, as the hacked celebrities experienced.

Apple's Challenge – Apple, Google, and other cloud providers now manage many of the most private and important aspects of our lives. We trust them with an astonishing range of information that, in some cases, has direct monetary value. They are, effectively, banks.

Securing a bank isn't easy. Account takeovers still occur on a regular basis, but, based on my experience, at a rate far below most online services. Banks deploy a wide range of security tools with names like "risk-based authentication," "user behavioral analytics," and "anti-fraud analysis." These tools catch many account takeover attempts, but not all, and financial institutions spend more on security than any other vertical market by a wide margin.

Some of the criticism I saw of Apple after the celebrity photo theft was warranted. It didn't appear that Apple used expected detection and analysis techniques for a cloud provider of Apple's size and importance, based on the effectiveness of the brute-force tool (even if it wasn't used in those attacks). Two-factor authentication (your password plus a code sent to your phone) was not applied to most iCloud services and was surprisingly complex to set up. Nor did Apple send activity notifications that could

have alerted a customer that someone had accessed her account and restored her data.

Apart from missing the brute-force attack vector, Apple's security team likely isn't to blame for most of these decisions. It is one of the best in the business but was clearly constrained by other considerations that can't be dismissed out of hand. Send too many user notifications, and they quickly lose meaning. Require two-factor authentication too frequently and users will revolt. Still, these were concerns I had even before the incident — I always worried that no matter how strong my password, my data could be exposed to an account takeover. I wouldn't even use iCloud backup for some of my devices.

Many of the criticisms and proposed solutions were naive. Numerous writers suggested mandating two-factor authentication. That's fine for someone like me with multiple iPhones and iPads, plus a wife I trust. But what if you have only a single iPhone and no one you trust to recover your account? Email password resets were another option, but what happens when the associated email account is compromised or is accessible only from the device you've lost? Go to an Apple store with an ID? That's fine for urbanites, but a massive inconvenience for a large swath of the population.

Hundreds of millions of customers use Apple products. I don't know what the iCloud numbers are, but we are talking about a company that sold 10 million iPhones in a weekend. Security complexity increases exponentially as fringe situations encompass millions of users. With Apple operating on that scale, the rules change.

Even behavioral analytics (identifying deviations from normal behavior through big data and automatic analysis) fails at some point. Take our celebrities, who may use their devices from 10 countries in 10 days during a press junket. They would likely have been excluded from the rules that could detect an attack on most accounts.

Apple thus faces one of the most complex security challenges in society, and faces it at a scale only a handful of companies need to consider.

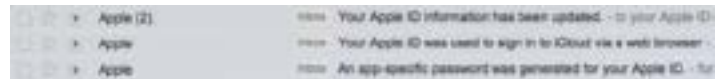
All In — Apple is fully capable of using its design and technical resources to tackle tough security issues. Touch ID is a masterful implementation of fingerprint technology. Apple approached the problem unlike anyone else, and simplified a complex problem to increase both usability and security without exposing privacy. Messages, FaceTime, and iCloud Keychain all leverage ingenious uses of encryption that are nearly transparent to the average user, yet still support more-complex options for those with greater security concerns. Gatekeeper effectively cut off the possibility of a widespread Mac malware market before it could grow. Apple Pay looks to be one of the most secure and simple payment systems ever implemented.

Contrast these with Apple's implementation of two-factor authentication, which is no better than anyone else's, and until recently quite a bit worse. It's one of those tremendously

difficult problems screaming out for an elegant solution. The company's response to authentication and account ownership requires a Touch ID-like rethinking of the problem. And to be clear, Apple is far from the first to tackle it.

Apple's initial response to the celebrity photo thefts closed the most significant gaps. Two-factor authentication, if you enable it, now protects everything related to iCloud. Since two-factor authentication breaks third-party software that relies on usernames and passwords alone, Apple also added the [capability to create secure application-specific passwords](#) that don't expose your entire account. App-specific passwords are bit of a hack — most other consumer cloud providers use a standard called OAuth instead — but moving directly to OAuth would break everything until developers could catch up. But Apple will need it eventually.

Apple is also sending more notifications for logins and changes to your account. This helps, but starts veering into a Windows Vista-level of notifications, especially with all the new device-level privacy notifications in iOS 8.



We don't know what Apple is doing on the server side, and likely never will. The company may be using a range of technologies similar to those used by banks. We do know it doesn't use risk-based authentication, which is the technology that causes your bank to occasionally ask you if you logged in from a trusted computer. I doubt that's the only gap.

I'm not about to tell Apple what to do, even speaking as someone who makes his living advising companies on cloud security. But I suspect there will be two basic facts about Apple's future cloud security moves:

- Apple will tackle the authentication problem, and likely attack it from multiple angles, all with a focus on simplifying a complex situation. No single approach has ever been shown to work at the scale at which Apple operates, so the challenge will be to simplify a range of options for different user demographics. Today Apple is, at best, average at this. With iCloud becoming the center of the Apple ecosystem, the company will need to break new ground. Even very few banks, if any, face the combination of internationalization, number of users, and diverse customer skills that Apple does.
- Apple will use every cloud security option in the book, and aggressively adopt new approaches and technologies on a continuous basis. It's the logical progression of a continual cat-and-mouse game as criminals constantly seek new ways of compromising user accounts. Apple has excellent server security, but account security requires different thinking and different tools.

At least I hope this is what Apple will do. One of my greatest fears is that Apple will focus more on trying to change user behavior, rather than improving the engineering of

the systems. In a [Wall Street Journal interview](#) Tim Cook said, "When I step back from this terrible scenario that happened and say what more could we have done, I think about the awareness piece, I think we have a responsibility to ratchet that up. That's not really an engineering thing."

My guiding principle as a security professional is: "Don't expect human behavior to change. Ever." No one, not even Apple, is about to eliminate the need for passwords or come up with a single, near-perfect way to protect

accounts. Nor can we rely on education or better security habits when hundreds of millions of users are involved. Apple most definitely had, and should have used, engineering options that could have reduced the chances of these attacks.

Apple just invested three years designing the first version of the Apple Watch. I look forward to seeing what the company can do with passwords and account takeovers once it truly focuses on the problem, assuming it chooses to do so. 🍏

November Software Review

FunBITS: Epic Zen Garden Shows off Your New iPhone

by Josh Centers

If you watched Apple's 2014 WWDC keynote, you might recall Tim Sweeney of Epic Games being brought on stage to show off his company's Zen Garden demo, which demonstrated the power of the new Metal API in iOS 8. His demonstration displayed amazing advances in shaders, artificial intelligence, and particle effects.

Now that tech demo, Epic Zen Garden, is available for free in the App Store. It requires iOS 8.0 or later on an iPhone 5s, iPad Air, or iPad mini with Retina display or later, and is a 232 MB download.

In terms of gameplay, Epic Zen Garden doesn't offer much, but if you just purchased a new iPhone 6 or iPhone 6 Plus, it's probably the flashiest way you can show off your new toy to friends.

Epic Zen Garden begins on the outside of a house, with three tappable targets, denoted by white circles. Each target opens a different activity (all screenshots were taken on an iPhone 6):



- Chair: Tapping the chair zooms you out to view the floating island that your house was built on. There's nothing you can do here other than watch birds fly by, but it's pretty! Tap the white arrow in the upper left to return.



- Tree: Tapping the tree takes you to what appears to be a dead tree. But hold your finger over its withered branches, and flowers will bloom. Touch the flowers to make the petals fall, which is a neat demo of Metal's particle effects. Tap the side arrows to rotate around the tree, the circle in the upper right to reset the tree, or the arrow in the upper left to return to the main view.



- Zen Garden: Tapping the sand brings you into the Zen garden. Drag your finger along the sand to rake it.



- Fountain: Finally, there's the fountain. Tap the bamboo to release a swarm of butterflies. Touch the screen to have the butterflies gather at that point.



- Pool: Tapping the pool zooms in on the water, showing a large school of koi. Dragging your finger across the water will cause ripple effects that the koi will follow. From the pool, you can also see three more locations in the distance:



- Courtyard: The middle option takes you into a courtyard, where you can visit the Zen garden or the fountain.



That's it. Despite the name, there's nothing particularly epic here, other than the lush visuals and the promise of things to come. You may remember the open-world Epic Citadel, which demonstrated the prowess of the iPhone 4 and which later evolved into the more constrained, but incredibly popular Infinity Blade (for my review of the third installment, see "FunBITS: Show Off Your New iPad with Infinity Blade III," 8 November 2013).

Much as the "gameplay" of Epic Citadel was very different than its final commercial release, I don't expect that whatever the fleshed-out Epic Zen Garden becomes will bear much resemblance to the "gameplay" of its tech demo. But it will be exciting to see what Epic does with the newfound power of Apple's Metal API. 🔄

Apple Updates

OS X Yosemite 10.10.1 Update

Nov 17, 2014 – 311.8 MB

System Requirements

- OS X Yosemite 10.10

The OS X Yosemite 10.10.1 update is recommended for all Yosemite users. It improves the stability and compatibility of your Mac.

This update:

- Improves Wi-Fi reliability
- Improves reliability when connecting to a Microsoft Exchange server
- Improves reliability sending Mail messages when using certain email service providers
- Improves reliability when connecting to remote computers using Back to My Mac

iOS 8.1.1

Nov 17, 2014

System Requirements

- iPhone 4s or later
- iPad 2 or later
- iPad mini or later
- iPod touch (5th gen)

This release includes bug fixes, increased stability and performance improvements for iPad 2 and iPhone 4s.

Canon Printer Drivers 3.1

Nov 13, 2014 – 287.6 MB

System Requirements

- OS X Lion or later

This update installs the latest software for your Canon inkjet printer and scanner.

Thunderbolt Display Firmware Update 1.2

Nov 13, 2014 – 1.7 MB

System Requirements

- 10.9.4 and later.

This update improves reliability when connecting devices to the Apple Thunderbolt Display, and addresses a rare issue that may cause the display to go black.

Digital Camera RAW Compatibility 6.01

Nov 13, 2014 – 7.5 MB

System Requirements

- OS X 10.10 w/ iPhoto 9.6 or Aperture 3.6

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

- Canon EOS 7D Mark II
- Fujifilm X30
- Nikon D750
- Panasonic LUMIX DMC-LX100

Epson Printer Drivers 2.19

Nov 13, 2014 – 1.19 GB

System Requirements

- OS X Mavericks 10.9 and later
- OS X Mountain Lion 10.8 and later
- OS X Lion 10.7 and later
- Mac OS X 10.6

This update installs the latest software for your EPSON printer or scanner for OS X Mavericks, OS X Mountain Lion, OS X Lion and Mac OS X v10.6 Snow Leopard.

Canon Laser Printer Drivers 3.0

Nov 13, 2014 – 57 MB

System Requirements

- Mac OS X 10.7
- Mac OS X 10.8
- Mac OS X 10.9
- Mac OS X 10.10


This update installs the latest software for your Canon laser printer and scanner for Mac OS X 10.7, Mac OS X 10.8, Mac OS X 10.9, Mac OS X 10.10.

FujiXerox Printer Drivers 3.0 for OS X

Nov 6, 2014 – 49.1 MB

System Requirements

- OS X Yosemite
- OS X Mavericks
- OS X Mountain Lion
- OS X Lion

This download includes the latest Fuji-Xerox printing and scanning software for OS X Yosemite, OS X Mavericks, OS X Mountain Lion and OS X Lion. 

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 held at 6:30 p.m. on the 3rd Tuesday of the month at Bethany Village Retirement Center, 5225 Wilson Lane, Mechanicsburg, PA 17055