con

South Bay Apple MUG

Macintosh

May 2015

Monthly CUPFUL for South Bay Apple Mac User Group Members

Apple announces updates to Mac notebooks

MacBook Pro
The 13-inch MacBook Pro with Retina display now features the all-new Force Touch trackpad, fifth-generation Intel Core processors, next-generation Intel Iris Graphics 6100, and ultrafast PCIe-based flash storage. It's the ideal notebook for enthusiasts and professionals looking for fast performance in an incredibly compact and light design. From $1299. The 15-inch MacBook Pro with Retina display has the power to do even more amazing things. Fourth-generation quad-core Intel Core i7 processors let you make quick work of even the most complex tasks in professional apps like Final Cut Pro X, thanks to speeds up to 2.8GHz, 6MB of shared L3 cache, and Turbo Boost speeds up to 4.0GHz. And every model comes standard with 16GB of superfast memory. All of which means the 15-inch MacBook Pro is ready to take on whatever you can dream up, wherever your travels take you. From $1999. For more info: http://www.apple.com/macbook-pro/

MacBook Air
The MacBook Air line now features fifth-generation Intel Core processors, next-generation Intel HD Graphics 6000, and a Thunderbolt 2 port. And with all-day battery life, MacBook Air will go with you and stay with you the entire day. Whatever the task, new fifth-generation Intel Core i5 and i7 processors with Intel HD Graphics 6000 are up to it. From editing photos to browsing the web, everything happens ultrafast. And all that power is encased in an incredibly thin 0.68-inch unibody design that weighs only 2.38 pounds. 11-inch from $899. 13-inch from $999. For more info: http://www.apple.com/macbook-air/

April 29 Meeting

Do you hate passwords? They're too hard to remember, there are too darn many of them, they want them to be complex and all different but it's impossible to keep track of them all! Allison Sheridan, who has presented to us before, will show you how to conquer your passwords! If you can make it to this presentation, you'll leave with a clear path to how to make secure passwords, have quick and easy access to them, and be able to get to them from your Mac or iOS device. She'll even offer you choice on how to do this! To accomplish this lofty goal, she will be demonstrating two password managers, 1Password and LastPass.

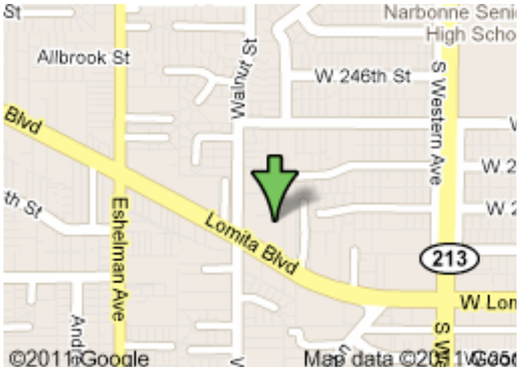
If you haven't seen Allison present before, you'll find her entertaining and informative, never boring!

In This Issue

Welcome to the SBAMUG
South Bay Apple Mac User Group

Meetings: Lomita Veteran's Hall,
1865 Lomita Blvd, Lomita
Mail: PO Box 432, Redondo Beach, CA
90277-0432
Phone: (310) 644-3315
Email: info@sbamug.com
Website: http://www.sbamug.com

Members,friends and colleagues are invited to attend our monthly meetings. The $35 annual membership dues entitle you to receive this monthly newsletter by mail or online, plus many more benefits (page 8). To become a member or get more info please check our websiite.



Lomita Veteran's Hall,
1865 Lomita Blvd, Lomita

SBAMUG Monthly Calendar

April 29: Password Play Date
May 27: iOS Apps

SBAMUG Meeting Format:

6:30—7:30 p.m. Questions & Answers and Sharing: *Everyone* is welcome, beginners encouraged
7:30—7:45 p.m. 'iSocial' – shoot the Mac breeze with others over a cookie
7:50—9:00 p.m. Announcements and Program

***Refreshments provided; donations appreciated!*

Submit suggestions for topics or speakers, or articles, ideas & original artwork for this newsletter by the last Wednesday of each month. Articles may be edited to fit space. Submit to: pjmyerz@gmail.com

Officers & Volunteers:

President: Clarence Baisdon   VP: Kent McDonald
Secretary: Wayne Inman   Treasurer: CW Mitchell
Directors at Large: Dave Nathanson, Margaret Wehbi, Pam Townsend, Glen Terry, Arnold Silver, Fran Pullara
PD Disk Editor: Jim Pernal
Membership: CW Mitchell
Member Development: Pete Myers
Programming: Kent McDonald   Greeter: Vacant
Server Director: Dave Nathanson
Newsletter: Pete Myers, Bill Berks
USPS Liaison: CW Mitchell
Refreshments: Member contributions

Other Meetings:

- 1st Wed each month – SBAMUG Core Group, 7:30 pm. Join Google+ SBAMUG community, or email: info@sbamug.com.
- Special interest groups (SIGs): Ask at the meetings or email: info@sbamug.com
- Last Sat. each month - Northrop Grumman-Ham Radio & Computer Swap Meet, 7--11:30 a.m. Meet at SE corner of Marine/Aviation Blvd, Redondo Beach
- Los Angeles Portable Users Group: Mac OS X, iPhone, iPod, MacBook, etc., http://www.lapug.org/

Membership Report – 111 members!

Please wear membership card as your name tag

Welcome New Members:

Thank You Member Renewals: Barbara Mathieu, Gundula Schneider, Frank Scholz, Paul Walesky, Amy Wasserzieher, Carol Simoes, Milan Korach**.**

If your name is not spelled right or your expiration date is wrong, contact cwmitchell@sbamug.com for correction. Or contact CW for everything membership, dues and benefits. Please watch for your renewal letter, then sign and date it and return it with $35 check or bring letter with payment to meeting.

THE SOUTH BAY MUG (ISSN 1058-7810) is published monthly for $35 per year by South Bay Apple Mac User Group, 2550 Via Tejon, Suite 3J, Palos Verdes Estates, CA 90274. Periodicals postage paid at Palos Verdes Peninsula, CA and at additional mailing offices. POSTMASTER: Send address changes to THE SOUTH BAY MUG, P.O. Box 432, Redondo Beach, CA 90277-0432.

SBAMUG April 2015 PD CD

This is the April CD article. Seven programs this month. Two programs are for Yosemite 10.10 only. I don't know if this is a trend or not.

a800d.zip The program name is AcaStat, a statistics program with data analysis. Takes in tab delimited or spreadsheet input. Can perform lots of statistical functions like regression and anova. OSX 10.7 Intel+. $19.99.

ABFRX9-3.dmg A "better finder rename" If you caught my talk on Yosemite that can now do batch renames of file names, I mentioned this program. Can do a lot more. Handles files, photos and MP3s. For photos this program can look in photos EXIF data and extract and apply the date the photo was taken. You have a lot more flexibility on renaming such as roman numerals. OSX 10.7 or greater. Intel Shareware. $19.95.

Classic Lava Lamp.zip A widget aka dashboard app that emulates a classic lava lamp. OSX 10.6.8+ Intel. Free.

Itsycal.zip This is a tiny calendar that lives on your menu bar. Displays calendar and can show appointments as a companion to Apple's Calendar program. OSX 10.10 Intel. Free.

Monolingual-1.6.5.dmg With bigger hard drives these days this program may be in less demand. Removes unnecessary languages from your OS, and frees up several hundreds worth of megabytes in your hard drive. Intel OS X 10.10 Yosemite only. Free.

SeaMonkey 2.33.1.dmg This is an alternate web browser. Based off the same engine as Firefox, it adds in IRC chat, HTML editing, Email and newsgroup reader as an "all in one" browser. OSX 10.6+ Intel. Free.

teleport.zip Free utility program to let you use a single keyboard and mouse to control multiple computers. OS X 10.7+ Intel. Free.

See you at the April meeting. PD CD will be the combined March-April one, available at the April meeting.

Jim Pernal, PD Editor

Google Cardboard, by Lily Prasuethsut

Fancy getting yourself a virtual reality headset but not sure which one? It's a bit early to actually buy one right now: most headsets, like the Oculus Rift, are developer's kits that cost a pretty penny. Others, like the Samsung Gear VR, don't have enough content and are pricey, too.

But there's one headset out there that is easily the most accessible, and also an arguably fun DIY project: Google Cardboard.Because all you're paying for is cardboard, a couple of lenses and maybe tape or velcro, the device barely makes a dent in your wallet. Google isn't selling kits anymore, but you can pick one up online for $20 or less from a variety of vendors. You can even download instructions to make your headset entirely from scratch.

Cardboard isn't for die-hard fans of VR. If you want to simply show people what the fuss is all about with virtual reality, Google provides a viable solution in the form of a cheap and portable product.

Despite being a Google-funded venture, the Cardboard is actually also compatible with iPhones. It simply depends on the availability of apps on the platform.Still, there are plenty of apps that work decently enough with Cardboard. Most are games that use Android devices, but more are being released for both Android and iOS. There are also VRSE-esque experiences like Google Earth or Photo Sphere, in which you are simply plopped into scenery much like a virtual tour guide.

Google's ingenious, little do-it-yourself project works better than I expected, considering it's just a piece of cardboard with two lenses attached, and then some. This may be basic virtual reality "tech," but there's definitely a certain appeal. The novelty of building your own VR device is a brilliant move. Coupled with cheap parts and untethered mobility, Cardboard is a great introduction for those skeptical about VR.

That said, do not expect the mind blowing experience of Oculus Rift, HTC Vive or Project Morpheus. Then again, it's not as if Cardboard is trying to be any of those. Rather, Google has cooked up an accessible piece of virtual reality that nearly everyone can enjoy. If you're on the fence about this whole "VR thing," then you have little excuse not to dive in.

http://www.techradar.com/us/reviews/wearables/google-cardboard-1287573/review

Photoshop at 25: A Thriving Chameleon Adapts to an Instagram World, by Farhad Manjoo

The history of digital technology is full of innovations that are praised for having changed the world: the Mac, Microsoft Windows, the Netscape Navigator browser, the iPod and countless others. Then there are the many products that changed the world and were suddenly overtaken by some newer, purportedly better thing: the Mac, Microsoft Windows, Netscape Navigator, the iPod and countless others.What's rarer in tech is the product that causes major changes, hits turbulence and then, after some nimble adjustment, finds a surprising new audience.

This week is the 25th birthday of one such aging chameleon, Adobe Photoshop, an image-editing program that was created when we snapped pictures on film and displayed them on paper. It has not just survived but thrived through every major technological transition in its lifetime: the rise of the web, the decline of print publishing, the rise and fall of home printing and the supernova of digital photography.

Photoshop attained the rare status of a product that became a verb, like Google and Xerox. Along the way, it became a lightning rod for controversy because of, among other things, the way it can be used to turn women's bodies into unnatural magazine-cover icons, or its use by propagandists and your casually mendacious social-networking buddies who doctor their vacation snaps. But now, for all its cultural cachet, Photoshop risks missing out on a far larger market of casual photo bugs and their smartphones. Once, for better or worse, we Photoshopped photos. Now, more often than not, we Instagram or Snapchat them, and everyone, it seems, is a photo editor. But not everyone needs or even wants a fancy program like Photoshop.

"When I took over the business in 2010, I realized that the growth in our business did not match what was happening all around us," said David Wadhwani, the executive in charge of Adobe's creative software. "Visual expression was on the rise everywhere. Our business was a solid business, but it was not growing at the pace that we felt it should." So Adobe is taking a big risk and reinventing Photoshop.

The process actually started in 2011. Rather than selling licensed copies of Photoshop and its other high-end creative applications for hundreds of dollars each (Photoshop used to sell for $700 a copy), Adobe began offering monthly access for as little as $10 a month. The price change was initially met with fury from loyalists, who didn't like the idea of renting rather than buying. Because subscription revenue comes in over time, the change also took a toll on Adobe's bottom line. Its annual net income declined 65 percent in 2013, and it fell 13 percent last year. But the company sees the decline as the short-term cost of a long-term plan. By lowering the price of Photoshop, Adobe hopes to democratize access, gaining new users who, in the past, wouldn't have been able to afford $700 software.

The trend looks promising. Adobe now has 3.5 million subscribers to its Creative Cloud suite of apps (which includes Photoshop), and it expects to have nearly six million by the end of this year, with annual revenue generated by those subscriptions approaching $3 billion. It's on track to beat the record $3.4 billion that Adobe made from selling boxed software in 2011.

Adobe also has grander plans to break up Photoshop into a number of apps, some of which it will make itself, with others made by third-party developers who will have access to Adobe's image-processing systems online. In some cases, those apps will even be free.

"The goal is to go from tens of millions of people benefiting from the technology within Photoshop to hundreds of millions of people over the years," Mr. Wadhwani said.

Adobe's move to apps and the cloud has earned plaudits from optimists on Wall Street. To understand why, it helps to understand Photoshop's history.

Photoshop began as a way to procrastinate from working on a doctoral thesis. In the late 1980s, Thomas Knoll, who was studying computer vision at the University of Michigan, began creating a collection of image-processing utilities for his younger brother John, who was a digital-effects specialist at Industrial Light & Magic. The program, which the brothers named Display, kept growing, and soon many of John's friends at ILM were using it.

In 1988, Adobe agreed to buy the program, but it didn't really have high expectations. Adobe gave the brothers no extra resources to finish the software; the company didn't even require them to go to Silicon Valley to work on it. John remained at Industrial Light & Magic, dreaming up new features for Photoshop, while Thomas stuck it out in Ann Arbor, where he wrote every line of code in the first version.

"The end result was, I never did finish my Ph.D.," Thomas said. But after about two years, he did finish Photoshop. On Feb. 19, 1990, Photoshop 1.0 began shipping. It was an instant success. Over the next decade, Adobe sold more than three million copies.

Many of Photoshop's features were built as analogues to techniques that photographers had long been using in the darkroom, but what set it apart from competing image-editing programs was the way it improved on the darkroom. For early users, it was a mind-blowing experience.

"What was amazing to me was the ability to change your mind all the time," said Maggie Taylor, a photographer whose painterly, collage-heavy art relies strongly on Photoshop. "With film, I had to make a decision, make the exposure and you're done. And I was often disappointed," she said. "With Photoshop, it's like, 'Wow, I can change my mind as many times as I want.'"

To the chagrin of some old-timers, Photoshop liberated photographers from the rigors of

continued on page 5

Photoshop, from page 4

physical perfection (and also from darkroom chemicals).

"In the days before a computer, you had to have very good hand-eye coordination to do photography well," said John Maeda, a designer and former president of the Rhode Island School of Design. Photoshop changed that.

But more important than what Photoshop did was the way Adobe navigated its market. In 1990, getting a photograph in and out of a computer was difficult because scanners sold for tens of thousands of dollars and printers and monitors had little capacity to produce high-resolution images.

The people who could get the most out of Photoshop, then, were designers working for newspapers, magazines and other industries that used presses.

"But we were always watching the trends to see exactly what features were required as the market evolved," Thomas Knoll said. Each time some new opportunity came along — from the web to inkjet printers to digital cameras — Adobe quickly tuned Photoshop to the new technology. Each time, Photoshop grew.

In a way, then, Adobe's turn to cloud-based subscriptions and mobile apps is similar: The business of software has changed, and Adobe is again shifting with it. Adobe now offers some of Photoshop's best features to outside developers, who can add advanced image-editing capabilities to their apps at no cost. Adobe is also building a suite of apps that offer specific cuts of Photoshop and other programs to a wider range of users.

"When I see all this happening, I'm down with what they're doing," said Mr. Maeda, who is now a partner at the venture capital firm Kleiner Perkins Caufield & Byers. "I think the younger generation of designers is looking for new tools, and they don't care what device it's on."

http://www.nytimes.com/2015/02/19/technology/personaltech/photoshop-at-25-a-thriving-chameleon-adapts-to-an-instagram-world.html?hp&action=click&pgtype=Homepage&module=mini-moth&region=top-stories-below&WT.nav=top-stories-below

Kindle Unlimited

Kindle Unlimited provides access to over 700,000 titles and thousands of audiobooks on any device for $9.99 a month.

Thousands of Kindle books come with the free professionally narrated Audible audiobook. With Whispersync for Voice, whenever you see "Kindle Unlimited with Narration," you can switch seamlessly between reading and listening without ever losing your place. Just pop in your headphones, tap the play button, and keep the story going...in the car, in the gym, in the kitchen, wherever your day takes you.
You don't need to own a Kindle device to enjoy Kindle Unlimited. With the free Kindle reading apps, you can read on any device with the Kindle app installed.

Two Step Verification in OSX 10.10

In addition to a new Photos app and emoji improvements, the developer release of the first OS X 10.10.3 beta also includes new direct support for Google's 2-Step Verification when setting up Google services in the Internet Accounts section of System Preferences.

2-Step Verification is an optional security setting that requires users to enter not only their account password but also a unique code sent by Google via phone app, text message, or voice call to a previously registered device or phone number, greatly enhancing account security.

Not all devices and apps support Google's 2-Step Verification, however, and as a backup Google also allows users to generate app-specific passwords to register a unique password for that device or app. The app-specific password can be revoked at any time by logging into the user's Google account for another time, making it easy to disable access on a device that has been lost or stolen.

On OS X 10.10.2 and earlier, users setting up their machines to access Google accounts with 2-Step Verification enabled have had to use this app-specific password option. Users trying to log in with their standard Google account passwords are met with error messages informing them they need to use this option.

But as noticed by developer Jonathan Wight, the new OS X 10.10.3 beta now fully supports 2-Step Verification, allowing users to log in with their standard passwords and unique verification codes.

The change makes logging in with 2-Step protected accounts much simpler and increases security by making sure the user attempting to log in has a secondary trusted device to provide the verification code.

http://www.macrumors.com/2015/02/06/os-x-10-10-3-google-2-step/

BlameThe Banks For The SoCalled Apple Pay "Fraud", by Patrick Moorhead

It has been a big year for Apple Pay. With 100s of thousands of supporting banking institutions and locations, it looks like Apple Pay has the momentum to succeed where Google (Wallet) and the telcos (Softcard) have so far failed. Apple's level of success to this point has been driven by three vectors: simplicity, privacy and security. But Apple Pay's security has been questioned in the past ten days in a few articles that appear to lay blame on Apple for not securing Apple Pay. The problem here is that the facts don't point the finger at Apple, the facts point directly to a few banks who aren't authenticating cards as they should, as some banks are authenticating stolen cards and cards from stolen identities.

It's important to understand the Apple Pay credit card on-boarding and authentication process to understand where the ball is being dropped. Banks are actually the ones doing the authentication, not Apple, and each bank can have their own ways authorizing cards, just as they have different ways of credit card acceptance with different levels of fraud tolerance. Banks can authorize electronically, via phone or by text.

My bank, Bank of America , asked me to call in for Apple Pay authentication for one of my personal cards, but electronically let a business account debit card go through without a phone or text check. Bank of America obviously saw something it wanted to check out on the personal account so I needed to call in. That phone check could have been made based on a comparison between the data the bank had and some of the encrypted data Apple sent to the bank.

Unknown to most, Apple actually sends additional information to the banks to help with authentication as outlined in the Apple Pay Security and Privacy Overview. It says, *"…Then [Apple] sends the encrypted data, along with other information about your iTunes account activity and device (such as the name of your device, its current location, or if you have a long history of transactions within iTunes) to your bank. Using this information, your bank will determine whether to approve adding your card to Apple Pay."*

According to the Apple iOS Security Guide's section on Apple Pay, it very clearly states that in addition to location and iTunes activity, Apple encrypts and shares information like the last four digits of the phone number and the device name. The bank then determines if the card is approved for use with Apple Pay. All of this information can be helpful in verifying, but only if the banks use it and if they are not, they may have to fix their process as part of this. This additional information Apple sends to the banks makes a whole lot of sense to help improve authentication. For example, a bank may want to provide a higher level of authentication scrutiny on a user's card who just recently opened an iTunes account, whose phone numbers don't match the billing address, or are currently in a different country than the billing address states. These examples don't always indicate fraud, but could certainly prompt a second factor authentication like a phone call or text. Some reported fraud rates are claimed at 6%, well beyond the 1% industry average. I have found a few interesting things about this figure. First, not a single bank is on record discussing this. According to Apple Insider, the only people going on record so far are people who actually benefit from an Apple Pay competitor's success. Also, what does the 6% actually encompass? Is it for a specific time period, maybe a specific country? Specifics aren't available. And finally, think about this.... if Apple Pay were truly insecure, banks would drop it like a hot potato, right?

Where do we go from here? Security is a constantly changing animal, so Apple is obviously working with banks to make Apple Pay safer. In the mean-time, people should start doing their homework to better understand how the Apple Pay credit card authentication works and focus on the right companies, the banks. Banks have always owned the credit card authentication process, not Apple. If one of the banks has something to say, they should go on the record and share specific data. I don't think this will happen, though, as I think we are witnessing a CYA moment, and it's so much easier to blame Apple than take accountability for an authentication flaw.

http://www.forbes.com/sites/patrickmoorhead/2015/03/17/blame-the-banks-for-the-so-called-apple-pay-fraud/?utm_campaign=yahootix&partner=yahootix

Can Your Car Be Hacked? A Fear That's More Hype Than Reality — for Now, by Doug Newcomb

A downside of our Internet-connected lifestyle is that the bits of data and personal information we access online potentially can be viewed by others, without our consent and without us knowing until it's too late. The hacking of connected devices such as computers and smartphones has become common, and no one is immune. No amount of security software and measures can keep hackers at bay if they want to break in badly enough.

Now that cars are becoming connected, they are also vulnerable to hacking. A recent segment on *60 Minutes* focused on cars, and the challenges of securing connected devices. It showed how a vehicle could be remotely hacked, causing the driver to lose control of essential functions such as braking. The day after the segment aired, U.S. Senator Ed Markey (D-Mass.) released a report concluding that automakers are not doing enough to secure connected cars and called for creating a federal rating system similar to the one for crash tests so consumers could assess the cybersecurity level when shopping for a new vehicle.

How real is the threat of connected-car hacking? How could it occur? Is there anything car buyers can do to protect themselves? And what are automakers doing to keep

continued on page 7

Car Hack, from page 6

connected cars secure? Here are some answers that separate the scare stories from the real situation.

Car Hacking: More Hype Than Reality

To date, there's been only one incidence of car hacking, and that was an inside job by a former car dealership employee in Texas who had access to a system that allows the repossession of cars by disabling the ignition system or honking the horn to embarrass owners who are behind on loan payments. Most other documented car hacks, including the one on *60 Minutes*, were performed by researchers, primarily as part of the Pentagon's Defense Advanced Research Projects Agency's (DARPA) work in the area of cybersecurity.

Nevertheless, "it's becoming a really big concern," says Thilo Koslowski, who covers auto technology for the consulting firm Gartner. "I do expect that some companies may take this too lightly, and this could lead to some very bad news for the auto companies and consumers."

"Cars themselves are not designed to fend off modern cyberattacks," adds Andreas Mai, director of Smart Connected Vehicle at Cisco Systems. But Mai, along with another automotive software engineer, a car security researcher and an analyst interviewed all say that while cars are just as vulnerable as any other connected device, the recent news reports surrounding car hacking are more hype than reality at this point.

Remote Hacks Are Feasible

While the researchers featured on *60 Minutes* didn't reveal how they gained access to hack the vehicle, experts interviewed believe they had physical access to the car via its onboard diagnostic port (OBD-II). This is the port that mechanics plug into to determine the status of a vehicle and detect problems, and that's a way of accessing a car that's consistent with another high-profile project funded by DARPA. In that case, a pair of researchers tapped into a car's onboard OBD-II port to take control of the brakes, acceleration and other critical systems.

According to Damon McCoy, an assistant professor in the computer science department at George Mason University, the hack seen on *60 Minutes* "replicated and extended, in some ways, our original research," which McCoy conducted alongside colleagues from the University of Washington as part of work by the Center for Automotive Embedded Systems Security (CAESS). The CAESS team said in its published findings that it wanted to "discover [whether] remote exploitation is feasible" and reported that the team was also able to gain access to the vehicle's electronics "via CD players, Bluetooth and cellular radio."

McCoy said that while CAESS found remote hacks are feasible, he added that, "the resources required...are much steeper" compared to being hard-wired into the vehicle via the OBD-II port. "They require a much larger scale of reverse-engineering effort to find those types of vulnerability."

Isolating Critical Safety Systems

Even if a hacker does gain access to a vehicle either by hard-wiring into the OBD-II port or accessing it wirelessly, a car's electrical system is designed to prevent breaching of critical systems.

The electronic architecture of cars today is such that it's "exceptionally difficult to do the levels of hack that some people are envisioning," says John Ellis, formerly global technologist at Ford and now head of the consultancy firm Ellis & Associates. "Safety critical systems — the brakes, the engine, the powertrain — are isolated," he says. "They don't intercommunicate."

Fixing Bugs Over the Air

Ellis agrees that cars could become more vulnerable to hacking as they become more connected and as automakers rush to add features in order to stay competitive and keep pace with consumer electronics.

"The biggest concern I have is the speed and adoption by automakers of technologies such as over-the-air software updates" that are prevalent in other connected devices, he says.

But these same over-the-air (OTA) software updates can also be used to plug holes in the security of a connected car, as BMW recently proved. ADAC, the German equivalent of the American Automobile Association, recently found that it was possible for a hacker to lock and unlock a BMW's doors by communicating with the embedded SIM card that provides the cellular connection for BMW's ConnectedDrive system. The issue affected about 2 million BMW vehicles, but the automaker quickly fixed the problem by pushing out an over-the-air security patch.

While it's clear that if you build a connected device, hackers will soon come and try to compromise it, some question whether they'll be inclined to go after connected cars. Currently, there's no strong monetary incentive. "The driver of hacking activities is profit," says McCoy.."

Taking the Issue More Seriously

If there's an upside to the intense and recent focus on car hacking, it's that it has made automakers take cybersecurity more seriously. General Motors, for example, recently hired a chief product cybersecurity officer, the first in the auto industry.

"I think we're talking about the issue before it's a real threat to most drivers on the road," McCoy says.

http://www.edmunds.com/car-technology/can-your-car-be-hacked.html?mktcat=nl-internal_standard&kw=driversednewsletter+main+tips+and+advice&mktid=nl80817172

PERIODICALS

SOUTH BAY APPLE MAC USER GROUP
P.O. BOX 432
REDONDO BEACH
CA 90277-0432

SBAMUG

Join, Renew or Give a Gift of a SBAMUG Membership!

For only $35/year you get:

- Monthly meeting program
- E-mail group help
- Monthly newsletter (We publish 11 issues per year!)
- Use our Wiki
- Free web space & e-mail on our server
- Build your own website
- Create your own blog
- Special merchant discounts
- $$$
- Occasional swaps, free software, raffles

http://www.sbamug.com/join.html
Or, contact Membership Chair
CW Mitchell at
cwmitchell@sbamug.com

SBAMUG Membership Application

South Bay Apple Macintosh User Group provides you with a local source of shared knowledge & experience through monthly meetings, trainings & monthly newsletter.

Individual & family membership: $35/year payable to SBAMUG
□ New Member □ Member Renewal

Name:____

Address:______________________________________

City:____________________ State:______ Zip:____________

Phone: (________)_____________________________

Email Address:_________________________________

Special interest:________________________________

Devices you use most:_________________________

How did you hear about SBAMUG:________________________

Comments:____________________________________

____

Signature:_____________________________________

Date: ______________________

Bring your Application and Fee to our General Meeting
at Lomita Veteran's Hall, 1865 Lomita Blvd., Lomita.
Or Mail to: SBAMUG, PO Box 432, Redondo Beach, CA 90277-0432