The PULP

HUGE this month:

General Meeting: June. 19th

Debut Video Capture Software & Raffle

See you there!

East Hartford Public Library
Main St. & Central Ave., E. Hartford, CT.

Q&A Session: 7:00PM–7:30PM
Meeting starts at: 7:30PM

Contents:

The Quiz	3
How to Tell If Your Cloud Provider Can Read Your Data	4
Stellarium	6
Flickr: A look inside the photostream	7
Calendar	10

Member of Association of Personal Computer User Groups APCUG

UGC

Apple User Group

The **PULP** is published monthly by and for members of the Hartford User Group Exchange, Inc. (**HUGE**). **HUGE** is a nonprofit organization whose aim is to provide an exchange of information between users of personal computers. The **PULP** is not in any way affiliated with any computer manufacturer or software company. Original, uncopyrighted articles appearing in the **PULP** may be reproduced without prior permission by other nonprofit groups. Please give credit to the author and the **PULP**, and send a copy to **HUGE**. The opinions and views herein are those of the authors and not necessarily those of **HUGE**. Damages caused by use or abuse of information appearing in the **PULP** are the sole responsibility of the user of the information. We reserve the right to edit or reject any articles submitted for publication in the **PULP**. Trademarks used in this publication belong to the respective owners of those trademarks.

MEETING LOCATIONS
East Hartford Public Library
Main & Central Avenue
in the Lion's Room
(downstairs)

Editor's Corner

June will feature the debut of 'DEBUT', video capture software. I'm, trying to figure it out and hope to have something ready for the meeting. There will be a ebook raffle.

In the news, rumors have it that Apple is about to revamp the iMac and Powerbook Pro lines.The WWDC is the first week of June. it's been about 11 months since the last new models, and some retailers have dropped prices on current inventory. Apple may drop the 17" Powerbook Pro. New models may include the new Intel Ivy Bridge' chipset. Also, there are some reports that an iPad mini (7" or 8") is on the way.

Apple has an update for a problem with the Lion upgrade. If you had 'Filevault turned on when you did the upgrade, your password could ber compromised. Do the update.

Apple has also update security for the iTunes/App store. You now have to select security questions & answers. Some of the questions posted on blog sites appear a little strange.

Adobe had announced that patches to some of its products (CSS) would require a paid update. That was recinded in about 48 hours. Microsoft is reported to be not including a DVD player in some of the versions of Win 8. You can either purchase it separately or use one of the products (VLC for example) currently on the market.

Some network enabled Samsung TVs can be placed in an endless on/off loop through some malware. Speaking of malware, can you guess whether a religious site or a porn site is more likely to infect your computer? According to Symantec, it's the religious site.

Tor Publishing has decided to stop using DRM for their ebooks.

Coming this fall to a theater (or TV screen) near you will be films shot at 48 frames per second.That's twice the current rate of 24. TV (iNTSC & ATSC) is broadcast at 30. It may smooth some of the blur in motions and allow for better 3D.

Remember the opening to 'Mission: Impossible' when the tape would go up in smoke. soon you may be able to do that with the RunCore self-destructive SSD. You can wach the video; --

http://www.youtube.com/watch?v=GLxaVFBXbCk

cont. pg. 9

Here is the appropriate copyright citation and a link to the full text. articles from "Tidbits"

http://creativecommons.org/licenses/by-nc-nd/3.0/

A Little Computer Quiz

by Stuart Rabinowitz

The trivia and minutiae of the computer related world. The answers will appear next month or you can submit an answer sheet at the General Meeting. Good Luck.

1 Clifford Stoll wrote a book about his attempt to catch a hacker in 1986. what was the name of the book?

2 Who was he working for at the time?

3 What was the name of the hacker he caught?

4 In 1995 someone hacked in the Citibank network and illegally transferred $3.7 million. He was caught and convicted, who was he?

5 Have you ever wondered what the US government 'really' knows about UFOs? So did an alleged hacker, who?

Answers to May, 2012 Quiz

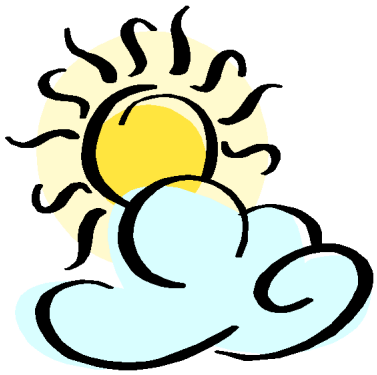
What was the first portable computer to use MS-DOS as the operating system and in what year was it introduced?
A 1982: The Compaq Portable

What was the first portable computer that could be recognized as a clamshell laptop and in what year was it introduced?
A 1982: The Grid Compass 1100

What was the first truly portable (battery powered) laptop and in what year was it introduced?
A Epson HX-20 announced in 1981 and sold in 1983

What was the first Apple laptop to be called 'Powerbook' and in what year was it introduced?
A The PowerBook 100 in 1991

What was the first laptop with a touchpad and in what year was it introduced?
A The powerBook 500 introduced in 1994



How to Tell If Your Cloud Provider Can Read Your Data

by Rich Mogull <rich@tidbits.com>
article link: <http://tidbits.com/e/12920>
2 comments

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

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

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

Practically speaking, multi-tenancy means your data is co-mingled with everyone else's on the back end. For example, with a calendar service your events exist in the same database as all the other users' events, and the calendar's code makes sure your appointment never pops up on someone else's screen. File storage services do the same thing: intermingling everyone's files and then keeping track of who owns what in the service's database. Some, like Dropbox, will even store only a single version of a given file and merely point at it from different owners. Thus multiple users who happen to have the same file are technically sharing that single instance; this approach also helps reduce the storage needed for multiple versions of a file for a single user.

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

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

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

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

<http://www.wired.com/threatlevel/2011/06/dropbox/>

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

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

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

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

1. Encrypt all the data for all users using a single key (or set of keys) that the cloud provider knows and manages.

2. Encrypt each individual user's data with a per-user key that the _cloud provider_ manages.

3. Encrypt each individual user's data with a per-user key that the _user_ manages.

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

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

Option #2 is a bit more secure. Encrypting every user's data with an individual key reduces, in some cases, the chance that one user (or an attacker) can get to another's data. It all depends on where the attacker breaks into the system, and still relies on good programming to make sure the application doesn't connect the wrong keys to the wrong user. It's hard to know how many services use this approach, but when done properly it can be quite effective. The major weakness is that the cloud provider's employees can still read your data, since they have access to the keys.

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

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

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

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

* If you can see your data in a Web browser after entering only your account password, the odds are extremely high that your provider can read it as well. The only way you could see your data in a Web browser and still have it be hidden from your provider is if the service relied on complex JavaScript code or a Flash/Java/ActiveX control to decrypt and

cont. on pg. 8

Stellarium

By Cal Esneault, President of the Cajun Clickers Computer Club, LA and leader of many Open Source Workshops & SIGs
December 2011 issue, Cajun Clickers Computer News
http://cccclinuxsig.pbwiki.com
www.clickers.org
ccnewsletter (at) cox.net

In my youth, I would take a copy of my uncle's *Star and Telescope* magazine and go to the center section to use the two-page star map guide. Twisting and turning the map to match my view, the many constellations and other night time wonders of the universe could be identified. Today, we can use vastly superior computerized versions to guide us through the night sky. One excellent program is *Stellarium*, an open-source program available for *Windows*, *Mac OS X*, *Linux*, and *BSD* operating systems. Although there are more sophisticated programs designed for professional and advanced amateur stargazers, *Stellarium* fits in the "fun" group by providing simple but detailed functions in a user friendly manner. The essential concept is to get an annotated view of a portion of the sky, adjusted for location and desired viewing time, which can be adjusted horizontally and vertically to match your viewing perspective.

Initial use can be confusing. It starts up in full screen mode with no menu items visible. Move your mouse to the left or bottom border to activate the command tool bars (see below). Those items on the bottom turn on the various viewing items (constellation names, constellation connectors, planet id's, horizon types, etc.). Those items on the left set up the system controls (location, time, item luminosity to display, etc.).

The default location is Paris, France. Go to the "Location window" icon to choose your city from a dropdown list (or input latitude and longitude). Next, go to the "Date/time window" to set your local time. By using up/down arrow controls you can see what the sky will look like at any future or past time (for example, what can I see if I go out tonight at 10:00 PM?).

Below is a screenshot of a night time view. I have added an azimuthal grid and constellation connectors. If you have a telescope with an equatorial mount, you can also display an equatorial grid. Clicking on any object will display key information (apparent magnitude, hour angle and declination, and azimuthal information updated for passage of time). Using the "ocular" view, you can see any listed object as viewed by a telescope of approximately 80x magnification.

The default system includes 600,000 stars along with a full Messier catalog of Nebulae. The constellations of 10 different

cont. on pg. 9

Flickr: A look inside the photostream
By Larry Klees, member, Orange County PC Users' Group, CA
October issue, nibbles & bits
www.orcopug.org
lklees (at) dslextreme.com

Once upon a time there were only a few photographers in an entire city. Today, thanks to advances in digital photography, there are only a few people in an entire city who are not photographers. When you factor in the internet; millions of photos fly around the world every second with the aid of numerous applications.

One of these applications that I personally like is called Flickr. Anyone with internet access can have a free Flickr account. A Flickr account is based on a thing called a "photostream." Photographs and short videos can be uploaded to this photostream which can be used like a personal photo album. The photos can be left in the order they are uploaded or they can be organized into sets like "Christmas 2010," "fireworks," "black sheep of the family," etc. These can be viewed and, if you like, downloaded or commented on by contacts, friends, and family members. Flickr allows you to place anybody in those categories and you can allow each category different access privileges to each individual photograph.

You can join special interest groups like "Bugs" or "Macro Photography" or "San Francisco," etc. If you don't see a group you like, you can even start a group of your own. You can use all manner of search criteria to find photos in your photostream or elsewhere on Flickr.

When you log on to Flickr you are sent to a Home/ Welcome page. This page gives you a quick summary of what has happened since your last log on. From this page you can monitor views of or comments others have left on your own photos; or you can take a quick look at the new things from your contacts, friends, family members, or groups. You can also upload new photos to your own photostream or organize other aspects of your account.

Flickr can be a little overwhelming at first but you will soon learn your way around. Flickr honors copyrights, doesn't sell your information, lets you control access to your photos, and offers many other security features. Many people like the free accounts. Many more like the extra benefits of the pro account for about $25 per year.

This space left blank unintentionally

from pg. 5

display the data locally.

* If the service offers both Web access and a desktop application, and you can access your data in both with the same account password, odds are high that your provider can read your data. This is because your account password is also probably being used to protect your data (usually your password is used to unlock your encryption key). While your provider could technically architect things so the same password is used in different ways to both encrypt data and allow Web access, that really isn't done.

* If you can access the cloud service via a new device or application using your account user name and password, your provider can probably read your data. This is just another variation of the item above.

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

<https://securosis.com/blog/how-to-encrypt-your-dropbox-files-until-dropbox-wakes-the-f-up>

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

<http://arstechnica.com/apple/news/2012/04/apple-holds-the-master-key-when-it-comes-to-icloud-security-privacy.ars>

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

Doing It Right -- The backup service CrashPlan is an example of a service that offers flexible encryption to fit different user needs, with three separate options. (For more on choosing the appropriate encryption method for CrashPlan, see Joe Kissell's "Take Control of CrashPlan Backups.")

<http://www.crashplan.com/>
<http://www.takecontrolbooks.com/crashplan?pt=TB1121>

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

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

Third and finally, you can generate your own per-device encryption keys, which CrashPlan never sees or knows about, rendering your backups readable only by you (or anyone who can beat the key out of you — never underestimate the power of a wrench — props to xkcd!). You could technically use a different encryption key on

each device (or share, your choice) so that even if one system were to be compromised, it wouldn't allow access to backups from your other devices. Clearly, this is much more difficult to manage and well beyond the needs or capabilities of the average user (heck, even I don't use it).

<http://xkcd.com/538/>

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

---

read/post comments:
<http://tidbits.com/e/12920#comments>
tweet this article:
<http://tidbits.com/t/12920>

from pg. 7

cultures are included. Various upgrade modules, plug-ins, and scripts exist (for example, you can expand to view over 200 million stars). Depending upon your needs, you can change the projected view of the sky - stereoscopic, fish-eye, cylindrical, etc. There is a text-entry search window quickly locate objects.

Download a free copy at stellarium.org (Linux users, find with your package manager). Smartphone versions are available for iOS (Android users, use Google Sky instead).

---

from pg.2

In a recent election in Palm Beach Florida, the optical scanning e-voting machines declared the incorrect winner for Wellington Village Council seats. Similar machines are in use in 300+ municipalities.

GM has unfriended Facebook, saying the ads got them no business. Google was found guilty of infringing on Oracle's Java copyright, but did not decide whether to award damages. They must first decide whether any patents were infringed. This could take awhile.

Verizon will be ending its 'unlimited data plans, even for those that were 'grandfathered'. How you might ask, by upgrading you to 4G or LTE.

Pystar, the Mac clone maker was denied an appeal to the US Supreme Court and the case is done.

Disney Research has developed technology to make almost anything into a touch device, including air & water. You can watch the video;

http://www.youtube.com/watch?v=E4tYpXVTjxA&feature=player_embedded

Stuart Rabinowitz, Editor

PULP Staff

Editor Stuart Rabinowitz
Distribution George Carbonell

Membership: Anyone may become a member. Dues are $12 per year and include a one-year subscription to The Pulp as well as access to the HUGE Public Domain disk libraries. Meeting topics, times and places can be found on page 1 of this issue.

Officers & SIG Leaders

President:	George Carbonell	860.568–0492	george.carbonell@comcast.net
Vice President	Stuart Rabinowitz	860.633–9038	s.e.rabinowitz@att.net
Secretary:	Ted Bade	860.643–0430	tbade@cox.net
Treasurer:	Charles Gagliardi	860.233–6054	epencil@att.net
Director at Large:	Richard Sztaba		richer1@aol.com
Web Manager:	Bob Bonato		wmaster@huge.org
Membership:	Richard Sztaba		richer1@aol.com
Integrated SIG:	Stuart Rabinowitz	860.633–9038	s.e.rabinowitz@att.net

June 2012

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					1 1867 Typewriter 1st described	2
3	4	5	6	7	8	9
10	11	12 1967 1st issue Computerworld	13	14	15	16
17	18	19 **General Meeting 7 PM**	20	21	22	23
24	25 1974 TI patents handheld calculator	26	27	28 Tau Day	29	30