# The PULP

## HUGE this month:

**General Meeting: Dec. 16th**
**This is a Tuesday !!!**

More Geek Gifts
See you there!

**New Location !!!!!**

**Knights of Columbus**
**2533 Main Street,**
**Glastonbury, CT**

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

Contents:



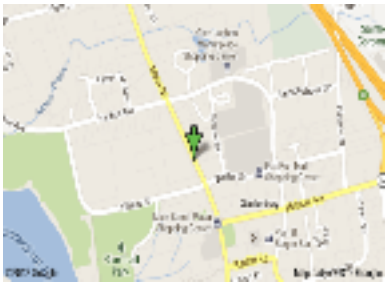
Member of Association of Personal Computer User Groups APCUG

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 LOCATION**
Knights of Columbus
2533 Main Street
Glastonbury, CT



# Editor's Corner

It's been an intriguing year of new & interesting geek products. In fact I've found enough to fill 2 meetings, so that's November & December. Also, in December, we'll talk about 'Little Snitch'.

In the news -- Microsoft has fixed a 19-year-old Windows bug found in everything since Windows 95.

Fujitsu announced that it can embed data in LED light that smartphones can detect. The system could be used to retrieve information about products on display or trigger a mobile payments system. The technology could also be used in museums, art galleries or trade shows.

AT&T has killed the 'permacookie,' and stopped tracking customers' Internet usage (for now).

The Internet Archive has a new arcade with 15 addictive video games for you to play.

https://archive.org/details/consolelivingroom

Intel is in the process of settling a civil suit involving P4 computers. The Important Deadlines:

| | |
|---|---|
| Deadline to Submit a Claim | April 14, 2015 |
| To Submit Request for Exclusion | December 15, 2014 |
| Deadline to Submit an Objection | December 15, 2014 |
| Final Approval Hearing | January 23, 2015, 9 a.m. |

Samaritans Radar is an app that mines Twitter for keywords indicating someone might be suicidal or "struggling to cope."

One lawyer may have just killed part of the

cont. pg. 9

# 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.

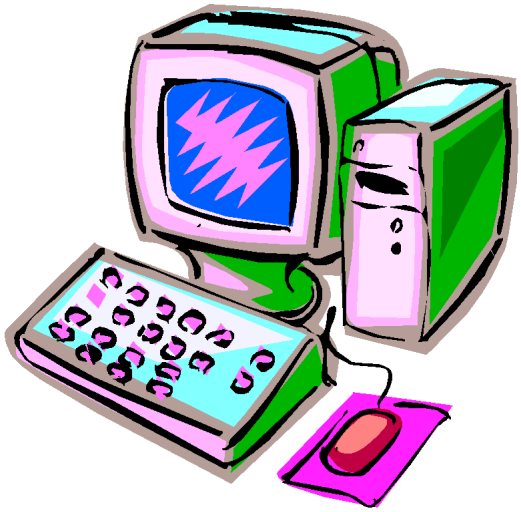
1 NeXt Computer developed the NeXTSTEP operating system, which is the precursor to OS X & iOS, but Apple was not the first company to license NeXTSYEP. What was the other company?

2 What was the first iApp developed at Apple?

3 Pixar has produced a number of fully computer animated feature films. What was the first?

4 In 1976 Apple began selling the Apple I through the Byte Shop, but they they sold one directly out of the garage. Who was that buyer?

5 What was the last computer based on the Apple II?



Answers to Nov., 2014 Quiz

November was an anniversary month for HUGE, so a few trivia questions --

1 Before there was a monthly quiz the PULP had another long running column. What was it called?

A Vaporware. The earliest version I have is 10/84 through 5/93

2 Who wrote it?

A Murphy Sewall

3 What was the best attended meeting held by HUGE?

A Broderbund, held at the Aetna in May, 1985 or maybe Guy Kawasaki

4 In 1989 Tim Berners-Lee hosted the first website on the World Wide Web at CERN. What computer did he use?
A He used a NeXT computer.

5 Where was the first website outside of Europe?
A At the Stanford Linear Accelerator Center

Smart Device Users Beware: Fraud May Be Just a Click Away
A Heads Up e-mail from the Southeastern Wisconsin Windows User Group
Reprinted with Permission from:
porte brown, Certified Public Accountants
www.portebrown.com / www.sewwug.org
email (at) sewwug.org

This was forwarded from a CPA Member of SEWWUG. Even if you don't have a described "smart device," it explains a lot about the QR Codes we often see.

You've installed anti-virus software to protect your personal computer and business network. You know the signs of phishing scams (including unfamiliar senders, poor grammar and misspelled words). And like most people who use the Internet today, you never open a suspicious e-mail or download files from a questionable website.

But what have you done to protect your iPhone, Android or tablet from cyber theft?

Many smart devices currently operate without anti-virus and malware protection. Although there haven't been many high-profile fraud cases involving smart devices, opportunistic hackers are targeting these devices as the world of quick response (QR) codes grows.

http://www.bizactions.com/img/Technology/lores_security_mobile_phone_code_safety_kk.jpg

Scammer's Delight

QR codes appeal to fraudsters for several reasons:

They're easy and cheap to create. All you need to do to set up a QR code is go to an online service and enter a web address. The site generates a QR code in seconds for free.

Malicious codes can be printed on stickers and placed on top of legitimate QR codes. Or a fraudster might post the code on a subway station bulletin board or a tourist monument and wait for curious victims to click on the image.

The human eye can't decipher QR codes. People can't tell a legitimate QR code from a malicious one. So it's easier to hide a "click jacking" scam than a phishing scam or virus. Smart devices don't usually slow down or show any other signs of "infection" until the user's data has long-since been compromised.

QR codes are relatively new, but rapidly growing. Hackers will increasingly exploit QR codes as more people purchase smart devices and more businesses use them for marketing purposes.

Users new to the QR code world may be unfamiliar with the risks of clicking on malicious codes and may not be security-conscious enough when using their smart devices.

What are QR Codes?

QR codes are square, two-dimensional barcodes that were originally used by auto manufacturers in the 1990s to track vehicle parts. Today, QR codes have become a popular marketing tool for businesses to connect with customers using smart devices.

You've probably seen QR codes in magazine ads, on business cards and product packaging -- even in taxis. Instead of remembering a web address and typing it into your browser, you can simply snap a photo of a QR code with your smart device.

Once clicked, QR codes perform all kinds of functions, quickly and easily. For example, a code might link to product specs on the company's website, enter the user into a prize contest, provide directions to an event, purchase a product using a PayPal account, "like" a company on Facebook or download coupons.

Unfortunately, QR codes can also be used to commit fraud.

Anatomy of a QR Code Scam

Some QR codes are self-contained. That is, all the product information is coded into the image. If you have a QR reader on your smart device, it auto-converts the image and directs you to a website.

Other QR codes require you to download or purchase an application (app) to access an online server, which looks up the desired information or performs some other function. Both types of QR codes -- direct and indirect -- are susceptible to fraud.

Scammers can, for example, embed shortened URLS into QR codes to misdirect victims to cloned websites, where the fraudster sells product without ever fulfilling the contract or installs malware to gain control over the device. The next time the user accesses his or her mobile wallet or PayPal account, the malware captures that information and makes fraudulent charges.

Alternatively, proprietary apps pose a security risk by allowing the QR code author to install measurement and tracking systems onto the smart device. Most QR code apps require consent to a user's agreement -- which many people fail to read -- and these could authorize the QR code author to track your cell phone usage, access your contacts and other personal information, or ring up charges for premium texts on your cell phone bill, for example.

An even bigger threat occurs when the user connects the smart device to a computer to charge it or sync data. The malware can "leap" to the PC, infecting it and any networks to which the computer is linked. This security risk is one reason some companies are leery of implementing bring-your-own-mobile-device (BYOD)

cont. on pg.7

Tiny Computers
By Dick Maybach, Member, Brookdale Computer Users' Group, NJ
November 2013 issue, BUG Bytes
www.bcug.com
n2nd (@) att.net

Personal computers are vital appliances for most of us. We use them to balance our checkbooks, calculate our taxes, communicate with friends and family, store our memories, and keep us informed. This is much different than when they were first introduced, when we felt free to perform experiments using them that today are unthinkable because of the risk of losing valuable data. As a result, we have the ironic situation that as our PCs become more and more complex, we know less and less about them. A solution is to acquire a smaller and simpler computer just to play with. Ideally, it won't take up much space on our crowded computer desk and will be cheap to replace if something goes horribly (or wonderfully, if you're adventuresome) wrong.

There are dozens of these tiny computers, but here I'll talk about just two, the Arduino and the Raspberry Pi. Both are supported by active on-line communities, both are described in several books, both are open source, which means you are free to make any changes you like to their software, and both are cheap - less than $50. (Although you will probably pay more for a complete starter or experimenter's kit.) Both were developed by educators, the Arduino in Italy and the Raspberry Pi in the UK, for the purpose of helping people learn about computers and computing. However, the two are quite different. The Arduino is really a controller, about as smart are your washing machine, and its inputs and outputs are Voltages on its pins. It runs only one program at a time, and once started, runs it forever. As you use an Arduino, you'll be learning programming and electronics. The Raspberry Pi is a real computer that runs Linux and comes with a full complement of PC software, including a Web browser. Its inputs and outputs are a keyboard, mouse, graphical display, and Ethernet and USB ports. As you use the Raspberry Pi, you'll learn programming, networking, and operating system operation and configuration.

The Arduino (http://www.arduino.cc/), like the Raspberry Pi, is about the size of a credit card. In the photo below, the Arduino is the blue card in the foreground. Normally, it's programmed and powered through the USB connector at the rear of the left edge. Once, a program has been loaded, it can be powered via the black connector at the front of the left edge (for example by a 9-volt battery). This unit illustrated is mated to a solder less breadboard, on which you can build circuits just by pushing component leads into its holes. Jumpers connect the breadboard with the Arduino's input/output pins along its front and rear edges. The Arduino is almost always used as a circuit element, and many experimenter's kits are available to get you started. These usually include an Arduino, a breadboard, and a collection of jumpers and electronic parts, e.g., LEDs, switches, motors, and sensors. Make an Internet search, and you will certainly find many interesting products and projects. My favorite vendor is Adafruit, but it has many fine competitors.

Getting started with the Arduino is quite easy. Go to their home page, http://www.arduino.cc/, and download the Integrated Development Environment (IDE), which is available for Linux, Mac OS X, and Windows. (Linux users can also find it in their repositories.) Connect an Arduino board to a USB port and start the IDE. As you may be able to tell from the screenshot, the Arduino uses a variant of the C programming language. The example here is the program blink, which just cycles an LED on and off. This is the equivalent of the classic "Hello World" program that is almost every C programmer's first effort.

The Arduino's capabilities are quite modest - typically the processor runs at 16 MHz, has about 20 I/O pins (some analog, some digital), and is equipped with 32 kbytes of EEPROM (for programs) and 2 kbytes of RAM (for data). Normally, you would use the Arduino just to control the hardware and send any data it collects to a PC for analysis. To make this easier, consider using the Processing language on your computer, available at http://processing.org/. It's very close to what the

Arduino uses and has an almost identical IDE.

You should be able to get started using only information available from the Internet, but if you prefer a book, look at *Getting Started with Arduino* by Massimo Banzi. Many others are available, some for the beginner and others describing advanced projects.

While the Arduino is a simple controller, the Raspberry Pi, http://www.raspberrypi.org/, is a real computer that uses the Linux operating system. The kit I purchased (from Adafruit) included a clear plastic case and a solder less breadboard, but many projects won't need the latter. The Pi has two USB ports (silver connectors on the center right), an Ethernet port (silver connector on the front right), a HDMI port for the display (silver connector on the center front), a power connector (micro USB connector on the front left), a SD connector for storage (a SD card protrudes from the case on the left), a collection of ports (connected to the breadboard by a black ribbon cable at the left rear), an analog video port (yellow connector at the rear), and a stereo audio jack (blue connector at the rear).

The Raspberry Pi is more powerful than the Arduino, with a 700-MHz ARM CPU and 512 Mbytes of RAM. (These specs are for the model B. The model A is much less capable and costs only a few Dollars less.) The processor is not Intel compatible; however, its overall performance is similar to a 300MHz Pentium 2, but with much better graphics. Clearly, it isn't an acceptable replacement for any modern home computer. However, it does act like a (slow) PC, as you can see from the screen-shot below, which shows the desktop with windows open for the Internet browser and file manager.

Getting a Raspberry Pi running is more involved than with the Arduino. Although it's powered through a USB port, PC USB ports can't supply enough current; you will need either a cell phone recharger or a powered USB hub. Be careful of cell phone rechargers though; many cheap units can't supply the current they claim. The safe approach is to purchase one from the vendor from whom you buy your Pi. You will need a USB keyboard and mouse; if you don't have an extra set, they are quite cheap. Hopefully, you have a HDMI display, either for your PC or a flat-screen TV; if not, you could try an old analog TV set, but its resolution will be poor. Finally, connect any USB peripherals through a powered hub, rather than ask the Pi to power them. I bought a no-name 10-port hub that had good user reports on Amazon, and it can also power the Pi. Finally, unlike the Arduino, which comes with its control software installed, you must supply the SD card for the Raspberry Pi and install Linux and its applications on it. This requires a SD card burner, and unfortunately many on the market aren't up to the job. Again, purchasing one from your Pi supplier is the safe approach.

As with the Arduino, you can probably get started with the Pi using only what you learn on the Internet, but there are also numerous books. The project has published *Raspberry Pi User Guide* by Eben Upton. There are numerous others, as well as magazine and Internet articles. I've seen descriptions of a media center, an Internet radio, a time-lapse camera control, a network file server, a firewall, and a wireless access point. (Many of these don't require a keyboard, mouse, or display once they are running, so you could disconnect these for use elsewhere once the project is on line.) You could even connect an Arduino to a Raspberry to obtain a portable sophisticated hardware control and data processing system.

Both these devices are ideal for experimenting. No matter how badly you screw up the software, you can just download a new program to your Arduino or reburn the SD card on your Raspberry Pi. Even if you manage to fry the electronics, you can replace either card for less than $50. Both are wonderful platforms for introducing electronics and computers to young people. There are many Arduino projects that can be completed in less than an hour, including building the circuit and writing the program. The Raspberry Pi software includes Scratch, a programming language for children that builds animated graphics with sound, and Python, a more sophisticated language for older kids and adults.

programs.

Users Provide the First Line of Defense

Surprisingly few iPhone, Android or tablet users have taken steps to protect against fraud. Here are four simple things you can do to protect your smart device starting today:

http://www.bizactions.com/img/Bullets/arrow_10x20_red_mb.gif
Never click a QR code in a public place, such as a bus stop or mall. Only scan QR codes from trusted sources or vetted by third parties. Be especially careful when traveling overseas where QR code "click jacking" scams tend to be more common.

http://www.bizactions.com/img/Bullets/arrow_10x20_red_mb.gif
Always check a QR code for a sticker before scanning it. Use your fingernail. If it looks like a sticker, it could be a scam.

http://www.bizactions.com/img/Bullets/arrow_10x20_red_mb.gif
Never provide personal information or passwords if requested by a website linked to a QR code, even if the site appears to be legitimate.

http://www.bizactions.com/img/Bullets/arrow_10x20_red_mb.gif
Install a QR code scanner app that screens URLs before directing you to the site. These apps block unsafe sites and stop online threats before they're downloaded to your device. Search for "secure QR reader" on your smart device. Read the reviews and select one from an anti-virus software provider you know and trust.

The end result of all this is simple: Your smart devices are personal computers. Treat them that way. Don't wait for a major cyber threat to occur to prove that smart devices are vulnerable to viruses and malware. Contact an information technology professional for more information.

The Smiley Face Turned 22 years old September 19th
Art Gresham, Editor, Under the Computer Hood User Group, CA
September 2013 issue of Drive Light
www.uchug.org
1editor101 (at) uchug.org

"Scott Fahlman was the first documented person to use the emoticons :-) and :-(, with a specific suggestion that they be used to express emotion. The text of his original proposal, posted to the Carnegie Mellon University computer science general board on 19 September 1982 (11:44), was thought to have been lost, but was recovered 20 years later by Jeff Baird from old backup tapes."

19-Sep-82 11:44 Scott E Fahlman :-)
From: Scott E Fahlman <Fahlman at Cmu-20c>

I propose that the following character sequence for happy:
:-)

Read it sideways. Actually, it is probably more economical to mark
things that are sad, given current trends. For this, use :-(

The information in the paragraph above is quoted from Wikipedia
http://en.wikipedia.org/wiki/Emoticon#cite_note-smiley-1

It is a very abbreviated summary of the story of how the keyboard characters we now call a Smiley Face came into existence. It is part of a much longer story of the inner workings of the earliest forms of computer to computer, and user to user communications, long before he internet as we know it. These 'Bulletin Boards' were first commonly used among academics. It all began as a rather prankish comment following this post on the Computer Science Bulletin Board System at Carnegie Mellon University.

"At around noon on September 16th, 1982, and in response to a similar scenario involving pigeons, Neil Swartz posted the following hypothetical situation to the CMU CS BBS:"

"There is a lit candle in an elevator mounted on a bracket attached to the middle of one wall (say, 2" from the wall). A drop of mercury is on the floor. The cable snaps and the elevator falls. What happens to the candle and the mercury?"

A very delightful reading of the complete story of the evolution of :-) is at
http://rhizome.org/editorial/2013/mar/13/emoticon1/
I am sure you will be ROFL when you read it.

Two Factor Authentication - Proof of Identity
By Phil Sorrentino, Staff Writer, The Computer Club, Inc., Sun City Center, FL
March 2014 issue, The Journal
www.scccomputerclub.org/
philsorr (at) yahoo.com

When you walk up to a teller in a bank and request information about your bank account, the teller may ask you to authenticate yourself by providing a picture form of identification. But if you have been going to this bank for many years and she is familiar with you, she may just give you the information. In truth, your face and her knowledge of you have provided the necessary authentication for her to respond to your requests. Authentication is much easier in the real world than it is in the software and computer-network world.

Authentication is the act of proving one is really who one says he or she is. In the computer world, we all experience this every time we sign on to one of our accounts or websites. Typically we are asked for a User Name and a Password. The correct User Name and Password combination proves, to the software requesting these items, that we are who we say we are. Of course, we could give our User Name and Password to a friend, something we rarely want to do because then he would be able to authenticate himself as the owner of our account. "Hacking" occurs when someone or some software program attempts to guess your Password after acquiring your User Name: maybe from some public information source. (Remember, User Names are available all over the internet.) This is a form of brute force "hacking" of an account. And unfortunately, there are many other, more sophisticated, ways of hacking into an account.

So, more formally, "Authentication is the act of confirming the truth of an attribute of a datum or entity, which might involve confirming the identity of a person or software program, or ensuring that a product is what it's packaging and labeling claims to be."

In other words, Authentication involves verifying the validity of at least one form of identification. As it turns out, practically, there can be three forms of authentication, called factors. Now, two-factor authentication requires the use of two of the three authentication factors. These factors are:

o Something only the user knows (e.g., password, PIN, pattern);
o Something only the user has (e.g., ATM card, email account, mobile phone); and
o Something only the user is (e.g., biometric characteristic, such as a finger print).

(These factors are so important for authentication that they are identified in government documents in the standards and regulations for access to U.S. Federal Government systems.) Some security procedures now require *three-factor authentication,* which involves possession of a password, and a physical token, used in conjunction with biometric data, such as a fingerprint, or a voiceprint, or a retina scan.

Two-factor authentication is not a new concept. When a bank customer visits a local automated teller machine (ATM), one authentication factor is the physical ATM card that the customer slides into the machine ("something the user has"). The second factor is the PIN the customer enters through the keypad ("something the user knows"). Without the corroborating verification of both of these factors, authentication does not succeed. Another example is when you use your credit card for a gasoline purchase and you have to enter your ZIP code to confirm the charge. You must provide a physical factor (something you own), the card, and a knowledge factor (something you know), the ZIP code. These examples show the basic concept of a two-factor authentication system: the combination of something the user knows and something the user has.

"Something only the user knows" is termed a Knowledge factor and is the most common form of authentication used. In this form, the user is required to prove knowledge of a secret in order to authenticate, typically, a password, PIN, or a Pattern. All of us are familiar with the password which is a secret word or string of characters. This is the most commonly used mechanism for authentication. Many two-factor authentication techniques rely on a password as one factor of authentication. A PIN (personal identification number), is a secret series of numbers and is typically used in ATMs. A Pattern is a sequence of things, like lines connecting the dots on the login screen of a cell phone or tablet.

"Something only the user has" is termed a Possession factor. A key to a lock is a good example. With today's computer systems your email account or your phone or a swipe-card is used as a possession factor.

"Something only the user is" is termed an Inheritance factor. Historically, fingerprints, a biometric method, have been used as the most authoritative method of authentication. Other biometric methods such as retinal scans are possible, but have shown themselves to be easily fooled (spoofed) in practice.

Two-factor authentication is sometimes confused with "strong authentication", but these are fundamentally different processes. Soliciting multiple answers to challenge questions may be considered strong authentication, but, unless the process also retrieves "something the user has" or "something the user is", it would not be considered two-factor authentication.

Two-factor authentication seeks to decrease the probability that the requester is presenting false evidence of its identity. The more factors used, the higher the probability that the bearer of the identity evidence is truly that identity. These systems ask for more than just your password. They require both "something you know" (like a password) and "something you have" (like your phone or email account). After you enter your password, you'll get a second code sent to your phone or email, and only after you enter it will you get into your account. It is a lot more secure than a password only, and helps keep unwanted snoopers out of your accounts.

Many well-known systems employ two-factor authentication. Some of these are: Amazon Web Services, Dropbox, Facebook, Google Accounts, Microsoft/Hotmail, Paypal/eBay, Twitter, and Evernote. The two factor authentication will typically be employed when you are using a different computer, or a computer from a different location, when trying to access one of your accounts.

Most of these two-factor implementations send you a 6 digit code via a text message for you to input when you receive it. This 6 digit code becomes the second factor to be used with the original password. This definitely adds an extra step to your log-in process, and depending on how the account vendor has implemented it, it can be a minor inconvenience or a major annoyance. (And it also depends on your patience and your willingness to spend the extra time to ensure the higher level of security.) But in the long run the use of a two-factor authentication improves the security of your private information, no doubt something we all want.

from pg. 2

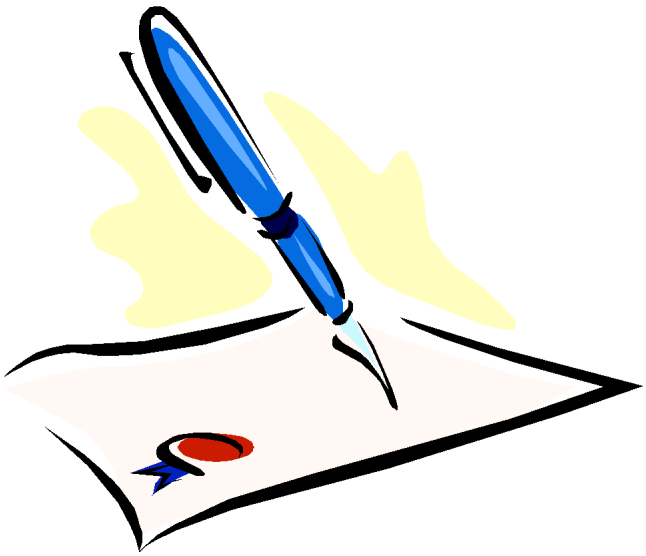
Internet of Things (IoT) because he found the intrusive nature of a smart TV in the 46-page privacy policy that came with his TV.

NASA creates first 3D printed object in space. It was a plaque.

Twitter has started peeking at the other apps on your phone.

A federal district court in Virginia has ruled that fingerprints used to lock a cellphone are not protected by the fifth admendment, but passcodes are.

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 |

# December

| Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday |
|---|---|---|---|---|---|---|
| | 1<br>1982 1st Intel 6" silicon wafer | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9<br>1968 demo of mouse | 10 | 11 | 12<br>1980 Apple goes public | 13 |
| 14 | 15 | 16<br>GENERAL MEETING 7PM | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26<br>1951 DPMA founded | 27 |
| 28<br>1969 Linus Torvalds born | 29 | 30 | 31 | | | |