



The Voice of FCUG

Happy New Year!

January 2007 Volume 27 No. 8

Contents

The Editor's Desk	2
Program	3
Questions and Answers - Chuck Davis	4
Tidbytes	6
Paradigm Shift in...Protection? - Vic Laurie	7
FCUG Party 5th December 2006	9
The Way We Were - January 1987.	10
Deep End - Cryptography - Mike Brotherton .	11
Digital resolutions ... - Dave Chrestenson . . .	14
A Lot of Assembly Required - Karen Rhodes .	15
CAPTCHA - Sandy Berger	18

**Meeting 7.30 pm 2nd at
New Canaan Historical
Society
13 Oenoke Ridge**

BOILERPLATE

"The Voice of FCUG" is the monthly newsletter of the Fairfield County Computer Users Group, Inc., a registered non-profit organization dedicated to helping members use their PC computers. Non-commercial and non-profit users are free to copy or quote material herein; proper credit and sending a copy of the publication to the Editor would be appreciated.

Members can exchange ideas and opinions through this newsletter, at a monthly meeting held the first Tuesday of most months, at occasional SIG programs, and on a bulletin board reached from the Club Internet Web-site at www.fcug.org.

Meetings and SIG groups are open to the public. Membership costs \$30/Yr, prorated. For information and payment contact

Ed Congleton, Treasurer: 203-966-4854,
251 Weed Street, New Canaan, CT. 06840

To submit articles or letters for The Voice send an e-mail message to wdhart@attglobal.net, hopefully with article attached, or mail paper, or even a diskette in ASCII, Word, or WordPerfect format to:

The Voice, 280 Main Street, Westport, CT 06880

The Editor's Mea Culpa

Two Editorial Errors are not a good way to start the year. The other day Alan quoted 'House', one of the many TV doctors, as saying 'everybody lies,' and it seems I am among the everybody.

Last month I said it seemed Nero, or Windows, had ignored my Linux disk partition and written over it. But, thinking about it, it seems more likely that it was another Operator Error.

A visitor was using the computer to copy a DVD and asked if the Windows D partition was OK to use. I said "If it's the large one of about 140GB, carry on." But that should have been the Windows E partition, and the name 'Windows D' was wrong; it pointed to my Linux partition. My question was correct and the visitor wrong – but the effect was the same. So I guess Nero, and Windows, were both blameless.

Also I have just fixed another mistake at last. My 140GB partition was formatted FAT32. But Microsoft (and others) say the maximum size FAT32 can use is 32GB. So I have at last redefined my 140GB partition as Extended, and broken it into several 30GB segments. Maybe life will be a little better now. . .





Program for 2nd January 2007

Call to order.Fearless Leader – Dick Booth 7:30

Novice topic: Searching the Web – Bill Hart 7:40
An Introduction to Search Engine logic.

Q and A: Guide – Thor K. Mada 8:00
He's not really a member, of course. . .

Epicurean BreakChef du Soir – Cookie Munster. 8:20
This one is an unknown, too!

Main topic: Computer Health – Mary Anne Franco 8:30
Using the Internet to supplement the work of your doctors

(Possibly followed by a raffle)

Adjournment. 10:00

LOOKIN' FOR A RIDE?



If anybody who wants to attend meetings has a transport problem, please mention it and together we will look for a solution. You can also contact Membership Chairman Lynn Bloom (203-380-9306, or lennyb2@optonline.net). She can tell you who lives near you, or might pass by on their way.

Questions and Answers

Chuck Davis

From the June 2006 issue of "Bits, PCs and Macs", the journal of the Sun City Anthem Computer Club of Henderson, NV

Question: I have created a form letter that I use frequently. The recipient's last name is used six times in the document. Is there a way to enter this once and have it appear in the other five places?

Answer: Yes. As is true in everything in computerland, there is more than one way. The best way to explain the techniques is to have you read the work of Microsoft Most Valuable Professional Greg Maxey. He has created an excellent article on his web site: http://gregmaxey.mvps.org/Repeating_Data.htm

If one of his solutions is workable for your situation, you might want to return and make a donation to help him maintain the cost of the site.

Question: You have extolled the use of the Windows XP backup program. Well, I have backed up the My Documents folder, but when I double click on the back up file, Windows asks what program do I want to open it. How do I get around this?

Answer: First you must understand that the backup file is a highly compressed file known only to the Restore function. Open the Backup Utility as if you were going to perform another backup. Once open you will see four tabs across the top of the dialog box. You may click on the Restore and Manage Media tab or click on the Restore Wizard (Advanced). Read and follow the instructions.

Question: I use Outlook 2003 for my email. I have placed both names and addresses for most contacts in the fields provided. I have been doing a copy and paste to place the addresses in Word's Envelopes and Labels. Isn't there an easier way?

Answer: Go straight to Word open the Envelopes and Labels dialog box. Notice the small book icon near the top. Click on that icon and select the mail recipient from the Outlook Select Name dialog box that opens. No cutting & pasting!

Question: I have just created a web site with many of my award-winning photos. Is there any way to stop people from using the images?

Answer: Nope! You will hear of a dozen ways that you can prevent copying your images, and you can spend days searching for additional ways to protect your images, but the harsh reality is that it can't be done. Of course, the surefire way is never put them on the web site.

Question: I have to prepare Microsoft Word documents for our organization and continue to be puzzled with paragraph numbering, numbered lists, etc. Can you give me a rundown on how to approach the subject?

Answer: The whole subject of numbering in MS Word is more than I want to include on these pages. I suggest that you download and save this 25 page treatise on the subject by Microsoft Most Valuable Professional John McGhie:

<http://word.mvps.org/Downloads/WordsNumberingExplainedUSLetter.pdf>

Question: I had absolutely nothing to do this morning, so I decided to check System Restore entries and found one called Software Distribution Service 2.0. I have absolutely no idea where that came from. I did an anti-virus scan

and came up with nothing. Do I have a problem?

Answer: The Software Distribution Service 2.0 restore point is created just prior to installing updates from Windows Update or Office Update. This is a normal restore point. Be glad that Microsoft has provided that function. The restore point is available if something goes awry following the installation.

Question: I have been having problems with my computer slowing down. Normally, I just reload windows and start fresh, but I have lost the product code. I really don't want to re-purchase the software. Is there a way to go into the program and find it.

Answer: First, I suggest that you solve the cause of your system bogging down. There is always a reason for poor performance. Two free programs are available to remove malware, spyware and adware:

1. Ad-Aware from this site:

<http://www.lavasoftusa.com>

2. Windows Defender (Beta 2) from Microsoft

<http://www.microsoft.com/athome/security/spyware/software/default.mspx>

Experience has shown that after you download and install these programs, most of your "bogging down" problems will usually go away!

There are several programs that will determine your product key, but the one that I recommend is called Belarc Advisor. It is a free download from:

http://www.belarc.com/free_download.html

In addition, the Belarc Advisor provides a complete inventory of your computer's hardware and software.

Question: I have heard that it's a good idea to clean the registry of everything that is unnecessary as a prophylactic measure. Can you recommend a good registry cleaner?

Answer: Some folks assume that these products are safe, because they have never had a problem with this cleaner or that cleaner. That's like assuming that it's safe to drive a car without a seat belt because you have not been hurt. I can't (won't) recommend any registry cleaner, because the registry doesn't need to be cleaned. Extra entries don't hurt your computer. Registry cleaners can get you in more trouble than any perceived prevention.

Question: I am using Word 2002 and Outlook 2002. When using Outlook with the Mail Format option set to "...Word to edit email messages.", then if I open Word and try to save a document, Word closes. If I open Word a second time, everything works correctly. I have already reinstalled Office with no change in this behavior. Should I buy Office 2003 to resolve this problem?

Answer: No! There are a number of reasons not to buy Office 2003.

1. Don't buy a three year old product when Office 2007 will be available in a few months.

2. As you have already learned, re-installation doesn't achieve anything useful. It doesn't affect the root of the problem which are your user files and registry entries. There may be several reasons for your problem. If you are running Norton AntiVirus or Norton System Works, there may be a conflict between their add-ins and Office. Some older versions of Adobe Acrobat and WinFax Pro may also be the culprits.

When Word is opened, several hidden temporary files are created, seemingly scattered around the hard drive. Open a document and more are created. Normally, these are closed when they are no longer required. However, if Word crashes and is unable to recover, some of the temporary files may be left behind to cause you myriad problems. This is the main reason Word documents become corrupt when

loaded directly from or saved directly to a floppy disk. Use your hard drive when opening and saving files. Then copy to and from the floppies.

For a complete discussion on this subject and detailed instructions to resolve your issues, see the following two articles:

1. What to do when Word crashes?
http://www.gmayor.com/what_to_do_when_word_crashes.htm
2. Problems opening Word (Word opens very slowly, or crashes (or gives an error message) as soon as it opens)
<http://word.mvps.org/FAQs/AppErrors/ProbsOpeningWord.htm>

Question: I'm using Office Outlook 2003. I also have a Yahoo email account. I can't send and receive the Yahoo messages from Outlook. Any suggestions?

Answer: You must have the premium (paid) Yahoo service to do what you would like. The product is called Yahoo! Mail Plus. You can read about this service at: <http://mailplus.mail.yahoo.com/help>

Question: No matter the program, when it is opened, the window is very small and I must click to maximize the window to read the information and work on the product. Is there a setting in Windows so that the window will open maximized?

Answer: No. That's because most folks prefer to have the windows take up less desktop real estate. You can achieve the same effect by dragging the corners with your mouse to the size that you want. Close the program. When you next open it, it will be the size as when you last closed it.

--o-o-o--

Tid Bytes

THINGS have not been well around the Editorial Desk recently. A whole new motherboard, with an Intel Celeron CPU instead of the Athlon 64. (He is sad, but it does apparently run at least as fast.)

Then he went to buy another Gigabyte of RAM and plugged it in. Wow! Two Gigs! And there was room for a third. His eyes began to glaze over. . .

But the other morning the machine refused to boot at all. Dead from the moment power was applied. Just like when the Athlon burned out. So back out for help; it had only been about three weeks since the new innards.

The expert did the stuff experts do: started pulling items off the power, one by one. Finally, the new memory strip – and peace was restored. So, for this month at least, there are only one thousand million little bytes holding these images as the Editor mashes my copy into the sort of shape he likes. . .

MORAL? When your machine fails, pull out things one by one, the newest first, until it works. Then you can put the rest back – one by one if you are being extra careful.



---ooOoo---

Do We Need a Paradigm Shift in Anti-Virus and Anti-Spyware Protection?

Vic Laurie

From the September 2006 issue of PPCUG News, the journal of the Princeton PC Users Group, www.ppcug-nj.org

Thomas Kuhn, a noted historian of science and my former faculty colleague at Princeton University, coined the expression, “paradigm shift”, to indicate the occurrence of a completely new and different way of looking at an area in science. Personally, I think that a paradigm shift is exactly what we need in the area of computer security. Fans of UNIX systems, especially Mac and Linux users, are going to immediately say that all that is needed is a switch to their favorite operating system. And they have a point. However, the Windows PC monopoly is not about to go away and the comments that I give here relate to the typical home computer user.

The present way of protecting computers against malware such as viruses, worms, Trojans, and spyware is basically reactive. It depends on a local database of information about known malware in order to recognize and disarm the invaders. Some attempt is made at using so-called “heuristic” techniques to recognize new malware that is not in the database, but maintaining the protection still requires constant updating of the local database. Also, since the different types of malware have different behavior patterns and signatures, more than one type of protection is needed. Although software suites may combine the different kinds of protection in one package, many people end up with a hodgepodge of different applications.

For example, I have an anti-virus program, a software firewall, a hardware firewall, three anti-spyware programs, an email filter, two Trojan removers, and various Internet toolbars for blocking popups, ads, phishing, JavaScript, etc. Having to run all these programs and having constantly to update them is not only cumbersome but also makes a hit on system performance. For example, Symantec products were such a drag on my system that I never ran them in the background but only used them manually. (I finally chucked Symantec’s Norton anti-virus in favor of AVG.) The fact is, even with constant updating, systems are still vulnerable to so-called “zero-day” and undocumented exploits. The constant parade of new security problems makes it clear that something better than the current approach to safeguarding computers is needed.

There are already several possible alternative ways to go. One is the procedure used on many systems that are open to the public in places like libraries and schools. A standard system configuration is established and any changes, including malware, that occur on the system during an individual login session are erased when the user is finished. The system is simply returned to its standard configuration. This approach has been very satisfactory in our classes at SeniorNet where we use the program Deep Freeze (<http://www.faronics.com/index.asp>). Students can do anything they want to the system or even get it infected by malware, but when it is rebooted it returns to its original pristine state. This is very satisfactory for a setup which remains static, but can be tedious where a user installs a lot of new software or frequently creates new files. Changes to the system can be incorporated into the standard configuration if desired, but this is a multi-

step process and not really suitable for dynamic systems where content changes frequently. However, this approach can be modified to add flexibility by having a separate unfrozen partition where data files and frequently changed programs are kept. Installations that require Registry entries will still need to be done in a multi-step process but the average home user who is an infrequent installer of new programs could certainly use this approach. Note that this procedure is much less time-consuming than restoring something like a Ghost image. Also, it is very important that the user does not have to do anything except reboot. A typical home PC user is not about to maintain up-to-date Ghost images.

A related approach that is attracting more and more attention is the use of "virtual" machines. The equivalent of several independent operating systems can be created on one computer. This is especially attractive for those who install or test a lot of software. David Berlind at ZDNet has an article on the virtues of VMWare. (<http://blogs.zdnet.com/BTL/?p=2462>) You can have one virtual machine that is the standard setup and another test machine that gets exposed to the Internet. If the test machine gets infected, it is deleted and the standard setup is copied. Creation of new data files on a virtual machine is no different from a regular computer. Installation of new software can be tried on the test machine first to make sure that the software is legitimate or has no undesirable effects. It is also possible to have a host machine that can access a virtual machine while the virtual machine is ignorant of the existence of the host.

At the moment, one problem with virtual machines is Microsoft's draconian licensing. They demand that two virtual Windows machines on the same computer pay for two licenses. This seems short-sighted to me. Microsoft has its own virtual PC software that it bought with Connectix and this is not a way to encourage its use. (Free download is at <http://tinyurl.com/eba5h>). Also this licensing policy seems likely to drive people into taking a look at Linux. There are ready-made Linux virtual machines available for downloading. I can easily imagine a setup where a Linux machine with its greater security is used for Internet connections while the more versatile, easier-to-use Windows machine is used for other applications. [Ed.Note: That is how I work at present.] The average home PC user may not be quite ready for the virtual machine approach but I think it is well worth considering.

Neither approach mentioned above requires a lot of defensive software with constant updates. It is not necessary to try to recognize large numbers of malware. Personally, I believe that approaches of this type combined with a good firewall are very promising. I do believe that a firewall is a must, since crackers are constantly probing for machines with open ports and the time it takes before you are likely to be attacked is too short. A firewall will keep intruders out and will also warn you if something does get on the system and tries to connect to the Internet. Note that the firewall responds to what something does, not what it is. This general type of protection is behind a new approach described next.

This different approach is mentioned in an article at PC Magazine (<http://www.pcmag.com/article2/0,1895,1911010,00.asp>). The company Sana Security has a program that monitors all running processes and examines suspicious behavior patterns. If it detects a process that it considers malicious, it quarantines files and Registry keys related to the process. According to PC Magazine, "Because it specifically responds to what a program does rather than to what it is, it is most likely to detect malware immediately upon installation or just after a system restart." It remains to be seen how effective this particular software will be, but the general approach of focusing on the behavior of software and not its specifics is the type of thing that should be pursued. A free trial can be downloaded at <http://www.sanasecurity.com/products/standalone.php>. This approach could

be the trend of the future but there are many companies with vested interests in the present way of doing things so there may be resistance from the Symantecs of the world.

A wildcard in all of this is the intentions of Microsoft. The company is moving steadily into the security software area. Noone outside of Redmond (and maybe not even there) can be sure about exactly how involved they are going to be in the security field. There may be anti-trust issues involved here so it isn't clear how far Microsoft may think it can go in incorporating new features that overlap with the products of other companies. However, security measures are a natural function for an operating system.

Finally, I have to mention the weakest link of all in the security chain: the user. If people used more common sense, it would solve a large part of the security problem. Without fertile fields of gullible suckers, spammers and phishers wouldn't find their scams worthwhile. If people thought twice about what they click on, all those worms wouldn't be propagating and my mailbox would be a lot emptier. I hope that I'm too pessimistic but I don't see a lot of hope here. I end with two quotes. The first is from MJ Ranum (http://www.ranum.com/security/computer_security/editorials/dumb/):

"There have been numerous interesting studies that indicate that a significant percentage of users will trade their password for a candy bar, and the Anna Kournikova worm showed us that nearly 1/2 of humanity will click on anything purporting to contain nude pictures of semi-famous females."

The second quote is from Neil Rubenking at PC Magazine (<http://www.pcmag.com/article2/0,1895,1980522,00.asp>):

"Even if there were such a thing as perfect protection against every attack, though, you're still [vulnerable]. As we used to say, the part of a car most likely to cause an accident is the nut behind the wheel. If you mindlessly obey e-mail messages like '*We am you bank. Fax to us you password for safeness,*' there's nothing any software can do to help."

---ooOoo---

FCUG Party 5th December 2006

The car parking facilities at Giovanni's were severely tested on Tuesday night. There were obviously several seasonal parties in progress on the same night. However, after a jam at the car park entrance for a minute or two, things went smoothly from then on.

Fortyfive of us settled down eventually to a delicious meal. (At least, your reporter's chicken marsala was wonderful, and the salmon and steak looked to be as good.) Small presents were laid at each place; nothing large and not all the same. And after the meal we received a second treat.

Pete Stair's talk, advertised as being about Manhattan, was really about the effect technology has had on civilization, with New York City as an example. The large-hulled square-rigged ships of the 15th century meant longer voyages were possible, as provisions and cargo could be carried – which led to the discovery of the New World. (The Vikings must have been really tough to do it in their open boats!) The printing press brought on more general literacy, and the printing of

maps encouraged exploration. Canals, steamboats and railroads cut freight costs and accelerated transportation -- and led to population shifts from the Old World to the New. The telegraph accelerated communication; what had taken three or more days now took only as many minutes. Elevators and construction steel allowed cities to develop upwards. Today's World-Wide Web and search engines like Google are already affecting our lives, and may do so yet in ways we have not envisaged.

Along the way we were introduced to a number of Knowledge Nuggets: Brooklyn was Dutch for Broken Land; The Bronx was Bronck's Farm; economic recessions were known as Panics until one president, asked if another Panic had commenced, said "No, this isn't a Panic; it's just a Depression!" Most of the other colonies had a religious underpinning at their starts: Jamestown (1607), the Church of England; Provincetown (1620), Congregational (as we call it today). But New York's religion has always been Commerce, and when the Dutch held it some 18 languages were spoken there in 1640. And when the British took it over the change was completely peaceful.

Anyway, you should have been there to have learned this (if your reporter has it right!) and a lot more; the audience were spellbound and the applause most appreciative at the end.

----oOo----



THE WAY WE WERE - JANUARY 1987

PRESIDENT:	Robert Jackson
VICE PRESIDENT:	Herman Parks
SECRETARY:	Patricia Brinson
TREASURER:	Aaron Bisberg
EDITOR:	Alan Abrahamson
TBBS SYSTEM:	203/.....

This Newsletter printed by Technical Reproductions Inc. Norwalk CT.

Shareware of the Month – AlanB.Abrahamson. Two disks; two pages.

Bill's Bumblings No.12 – Bill Hart. Three pages of Pascal.

Serendipity 11 – Lucien R. Greif. Eating near the Javits Center. One page.

A New Year – George Saladino. A miscellany in Three pages.

FCUG Minutes for November 4, 1986. Roger Giler on investing and Bill Hart on Linear Programming.

The Comm_Line – Dick Carricato. The history of communications in four pages.

Roger's Ramblings #15 Three pages on backing up.

January's Agenda – Herman D. Parks. Aaron Bisberg will show how to speed up Basic; Alan Abrahamson will discuss the Data Base Manager which was this month's shareware offering.

---ooOoo---

The Deep End – Cryptography

Mike Brotherton

In November we looked at some simple, manual ways of encoding messages to keep prying eyes out. We came to the conclusion that manual processes just weren't cutting it. So let's pick up where we left off...ready to attack the problem with computers, which should make things easier to encode and harder for others to break, right?

Enter the Computer:

Not exactly. Most programs, as noted before, use computer versions of the insecure algorithms we discussed last time, and hence they are insecure. That's why you can buy/download programs to generate passwords for password-protected Excel, Word, and WordPerfect files. Computer routines often use one key string (which immediately defines the periodicity of the code) and encrypt the cleartext with each successive letter in the key. These algorithms are often based on the computer command XOR (Exclusive Or) which compares two bits and essentially says, if the two values match, return 0, if not, return 1 – that is, one or the other, but not both. Also remember that all computer data is essentially 1's and 0's, so an XOR works the following way on two bytes of binary data:

Byte 1: 10101010

Byte 2: 11001100

Byte 1 XOR Byte 2: 01100110

Read the columns downward to see how the patterns react. Interestingly enough, if we take that result and XOR byte 2 against that result again, look what we get:

Byte 1 XOR Byte 2: 01100110

Byte 2 again : 11001100

1 XOR 2 XOR 2 : 10101010

We get byte 1 again! How cool is that? So, by using XOR as a function, one has a symmetrical cipher. That is to say, the same key you used to encode the message is used to decode the message as well! Unfortunately, pushing 'ABCWXYZ' through an XOR N (N being some number) process always produces the same results. All A's turn to some number X, and all B's turn to some number Y. Sound familiar? For all our efforts, we've re-invented the substitution algorithm – aided by the speed of computers. We already know that works for kid-sisters only (and lazy bosses). What if we change N (the value XOR'd against) for each character? Yawn. Been there, done that. That's the Caesar Cipher we talked about last time. That's easy to break too! No wonder Caesar is better known for his salads than his ciphers. ;-) Sorry, couldn't resist that one.

As stated before, if there is periodicity to the key, then the encryption is insecure. So, what if we feed the encoding routine a truly unique (ie random) value for each character of cleartext to be encoded -- a code which never repeats? Then a substitution code can be successful. However, the sequence of the key can NEVER be reused, otherwise you've introduced a period and that's the beginning of the end. If we start with our "random" key of "AGJHOEPT..." to encode message 1, and

then use it again against message 2, then we have created periodicity (the two messages each start the code from the beginning), which allows cryptanalysis to eventually crack it. So we have somewhat solved the problem but created two new problems. The first problem is that we have to generate a truly random value (or sequence of values), which is difficult to do with a non-random computer, and most “pseudo-random” number generation routines in computers do have some repetition or patterns which makes them not truly random. Using a similar system to decode would narrow the possibilities significantly. Of course, we could manually create the random list and feed it to the computer to get around that problem – tedious but possible. The second problem is that after we generate the ciphertext message, we have to somehow communicate that random sequence to the person doing the decoding so they can decode the message. Now remember, it’s not as easy as saying “The Quick Brown Fox” is the key used to encode the message. In order for the key to work, it has to be random, it has to be as long as the cleartext message, and it has to lack periodicity. Transmitting the key is not an easy task to do when you consider the key is as big as the message. So a 3MB file requires a 3MB key. Not particularly useful – in order to pass a secret message, you need to not only pass your secret message securely (which has been encoded as ciphertext in case it’s intercepted), but you also have to send the key to decode the ciphertext as well. And you certainly don’t want to put all your eggs in one basket (ie: by using one courier to bring both message and cipher key), so that means twice the work to send one message. Even if you ship a DVD’s worth of random key data to be used for decoding, it can only be used once, or else you end up with a “period” to your encoding and hence, you’re open to attack. There’s got to be a better way!

Let’s Get Serious Now:

After the Second World War, cryptography took a more serious approach to the problem, rather than the “clever” tricks of substitution and transposition. People turned to mathematics for a solution. Inside mathematics, there are plenty of functions with interesting properties which can be used to create ciphers. Two kinds of ciphers have come out of the mathematics-based approach are symmetrical and asymmetrical key algorithms. With symmetrical algorithms, the key used to encrypt the data is also used to decrypt the data, as we mentioned earlier – such as our XOR scheme. So in order to use this system of encryption, the key must be transmitted with the ciphertext or the key must already be known by the recipient. Some current implementations using symmetrical key algorithms are Kerberos, DES (Data Encryption Standard), and IDEA (International Data Encryption Algorithm). But again, the transfer of encryption keys is a limitation of these systems. At some point in time, the keys have to be passed around to all necessary parties.

Let’s think again, think about the situation. Even if you decided to use random keys, you’d have to distribute those keys to all of your recipients. So this means you have to know and trust your recipient, and have a safe means of exchanging the keys. You can’t send an encrypted message to a complete stranger because you first need to exchange key data either with that person directly, or through some sort of trusted intermediary. So is this the best we can do? Wouldn’t it be nice to limit the number of keys needed to be used? Wouldn’t it be nice if there was some way of publicly or openly passing keys to complete strangers without worrying about people intercepting the transmission and compromising the system?

Well, this is the beauty of asymmetrical key encryption, the heart of PGP (Pretty Good Protection) public key encryption. The idea is that a “key” really consists of two parts, a “public key” and a “private key”. The public key is just that,

public. You can post it on your web site for the world to see. Your public key is a key that anyone who wishes to send encrypted data to you will use to encode that data. On the receiving end, you have the matching private key. It is used to decode the ciphertext messages sent to you which are encrypted with your public key, regardless of who sent it to you. As long as the data was encrypted using your key, you can decrypt it. Now, as I said, this process is based on mathematics, not on substitutions or transpositions. The details of this math get a little hairy for most to understand, so let me oversimplify the problem so it's a bit more understandable. If you prefer hairy, go to <http://www.dongrays.com/btd/crypt-how.html>.

In order to implement our public/private key solution, we are implementing an asymmetrical key cipher. That is, the encoding cipher uses a different key than the decoding cipher. This way, we can give away one half of the key (the "Public" key), and retain the inverse cipher (the Private key) for decoding. Let's start by making life easier and switch to a numeric message since we all know that text is represented internally as numbers in computers. So, what we're looking for is essentially a function and an inverse to that function to apply to all the numbers in the cleartext message. I'll choose (again, this is oversimplified) my functions as $6x$ (six times x) and $x/6$ (x divided by six). So I tell everyone my public key ($6x$) and keep my private key ($x/6$) a secret. So, when someone is encoding data for me, they take each number and multiply it by six. Then, when I receive the document, I take each number in the ciphertext and divide by six to get the original cleartext. So, if your message to me is 1,2,3,4, you would send me "6,12,18,24" ($1 \times 6 = 6$, $2 * 6 = 12$, etc) as the ciphertext. On the decoding side, I'd use the $x/6$ function and get $6 / 6 = 1$, $12 / 6 = 2$, 3, 4! Now again, this is an overly simple function pair, and encryption functions are far more involved than this. But if I were to get some kind of mathematical function for which finding the inverse would be extremely difficult, then I'd be in business.

I would point out another issue to contend with in all our prior encryption schemes...the actual method of encoding is known. If someone knows HOW you encoded your data, that gives them a leg up on trying to figure out how to decode the message. So, even if they didn't know much about the message, if they knew you used program XYZ to encode your message, they could easily reverse-engineer the XYZ program, figure out HOW the data was being encrypted, and use that to help simplify the methods for attacking the message when trying to decode it. With mathematical-based schemes, the functions being used can be read from the software, but not the constants and parameters fed into the functions. With our prior example, they know the function is Nx , and x/N , but if they didn't know $N=6$, they'd have to work on figuring that out. With enough unknowns in our math function, knowing how the function works doesn't help without knowing the constants used for the particular instance. The beauty of the Public Key Encryption schemes is that they actually don't care if someone knows HOW it was encoded, because it is believed that even though you know the function used to encode, that someone doesn't know the parameters used, and hence they've got a lot of work trying to find out what the parameters were that generated the ciphertext.

So, now that we know the theory, what does this mean in practical terms? Is any of this available commercially? Is there a "plug-in" for my email client? The answer is, yes, there are. PGP software is readily available and ready to use today. In fact, for those who deal with certain banking and financial groups, you may already be forced to use it for data communications. So, next time we'll put this into practical application. We'll get ourselves some PGP software and have a go at it.

DIGITAL RESOLUTIONS MADE CONFUSING

Dave Chrestenson, Fox Valley PC Association, Oswego, IL

From the October 2006 issue of User Friendly, the journal of the Los Angeles Computer Society

There seem to be a plethora of articles on the number of pixels required to create your photos to their full glory. Many of the articles disagree with each other and some are mystifying (to say the least); occasionally a few are wrong. So here I will approach it from a different point of view; I'll give you the knowledge and let you decide what you need. Ready? Here we go!

Let's start with some facts. (I'll reconsider these later, but we have to start somewhere.) First, the average eye, relaxed, focuses at a distance of about fifteen inches. So that's about the distance people view their prints.

Second, the angle of comfortable vision (not acute) is generally agreed to be about fifty to fifty-five degrees. Beyond that is peripheral vision. Now, fifty degrees at fifteen inches subtends a distance of about thirteen inches, just covering the diagonal of an 8x10. Is it any wonder that size is so popular?

And third, the typical eye has a resolution of about one minute of angle. This works out, at fifteen inches, to about .004 inches, or approximately 229 dots in an inch. For purposes of clarity I will use the term pixels when referring to the camera sensor and dots when referring to the print. But in this discussion they can be considered equivalent. Don't compare this with the resolution (normally also referred to as dots) of printers. They are completely different animals.

For convenience, and to assure a tolerance, for now let's round that up to 300 dpi. This means that we need 300 dpi (at 15 inches) on the paper to assure that we won't see individual dots. Now, it's easy enough to work backwards from there. Assume that we wish to print an 8x10. Ten inches across at 300 dpi is 3000 dots. Eight inches down at 300 dpi is 2400 dots. So we need a camera of 3000 x 2400 pixels, or 7.2 meg. (This is assuming a camera with square pixels, not all have that. The Fuji S3, for example, has hexagonal pixels, two sizes, no less. (Subject for still another article?))

Simple huh? Maybe. But let's try another example first. Assume you just want to print a picture half that size, 4 x 5 is more common. Then 4 times 300 equals 1200 and 5 times 300 equals 1500, so our camera need only be 1.8 meg. That's not so bad, is it? But before you dash right out to buy a 2 meg camera on sale, let's take a look at some of those original figures.

I said that the average eye views an image at 15 inches. That's an "average" eye. It can vary from that... a lot. Depending on age, it can go from 3 inches (a youngster) to more than 6 feet. (An old timer.) And that's for an eye that's working well. Near-sighted? You'll hold the picture closer. (Assuming you don't wear correction lenses, of course.) Far-sighted? Further away. Have astigmatism? A mess! So, if you hold your picture at 7.5 inches, you will need twice the number of pixels, or 600, per inch. An 8x10 would require a 28.8 meg camera. Good grief! Thirty inches viewing distance is a lot easier, a 1.8 meg one will do the job. Also, some eyes can see significantly better than one minute of angle, some can reach 1/2 minute. That's even worse, you need 600 dpi at 15 inches, which means we're back to a 28.8 meg camera for an 8x10, and a 7.2 meg one for a 4x5. But you can do the math. And do you really need to have the dots as small as theory suggests? Well, to make it more confusing, there are other considerations that affect that. Bright lighting needs higher resolution, dim lighting needs less. Glossy paper? Higher resolution. Matt paper, less. High contrast image, more, low contrast, less. Ad

infinitum.

Finally, what if you have taken the definitive photo of Yosemite, the one to equal Ansel Adams, and you want to have it printed at, say, 16x20 and frame it. Do you still need 300 dpi? Probably not. After all, people don't normally hold a 16x20 in their hands and look at it from 15 inches. Remember the 50 degree vision. So, you'll probably be hanging it on the wall, where they will view it from a distance.

Experience shows that people will move backward or forward when viewing a picture until it subtends that 50 degree angle. So you might well get away with 150 dpi. But, getting back to the more normal usage, handheld prints, do you need 300 dpi there? Again, maybe. In many cases you may get away with less. But if you go below 150 dpi you are almost certain to get obvious visual pixilation at that distance. Of course, Photoshop to the rescue, you can resample upwards and increase the number of pixels to what works. You're not adding detail, but at least you're getting rid of those annoying "jaggies."

Clear? I didn't think so. Remember, I said "Made Confusing." But at least you are now confused on a much higher plane! Good luck.

---ooOoo---

A Lot of Assembly Required

Karen Rhodes

My computer died. It was old, in computer terms, and the motherboard had had it. It wasn't much of a task to get my data files off before it completely went west, as I keep most of my data on Zip disks or USB portable drives. But it was time for me to get a new computer.

It isn't my first choice to go to Gateway or Dell or Hewlett-Packard and buy an already-assembled machine. First, I want on my computer only the software I will be using, not some techie-nerd's idea of the latest "in" thing. Second, I don't want to have to go round and round with someone on the other end of a telephone about what components are available. The bottom line is that I want what I want when I want it, and nothing more – or less.

My preference for assembling is made much easier by having someone in-house who is experienced at it – my husband, who is a computer specialist. He does everything; he installs hardware, software, LANs, the whole works. There are some things he doesn't know, but he knows enough to be able to put together a computer -- one that works. He's done it before, for himself and for others, on the job and at home.

He did the shopping for me because I get lost when it comes to putting one part of the computer in concert with another, and knowing what is more likely to work with what. You notice I said "more likely;" there never is a guarantee that it's all going to work once you get it together!

Having done business with Newegg.com before, he settled on them. He gave me a list of recommendations. I ordered; the next week, we had all the parts. That next Saturday, after breakfast, the assembly began.

I'll go though the process he used, making what I think are some important points to remember (marked by bullets).

- **Don't always settle for the power supply that comes with your case.**

I ordered a mid-range case, which came with a 350-watt power supply. Probably not enough for my powerful and large genealogy database program and a lot of multi-tasking that will inevitably accompany its use, and certainly not enough

for the motherboard I bought, because I also play games for which I bought a powerful graphics card and a muscular motherboard. And the motherboard I ordered states in its manual that it requires a minimum of 400 watts in the power supply. I bought 550 watts.

- **If you do boost the power supply or you live in a hot climate (both apply to me), buy extra case fans. They're inexpensive, and the extra cooling they provide is crucial to computer health.**

The case came with one fan installed. My husband put in the two extra case fans first. Then he put in the power supply (Just PC model JPC-550C-12V). Next he put onto the motherboard (EPOX EP-8 NPA) the CPU (AMD Sempron 64 3100+), the memory (Corsair, 1 GB), and the Graphics card (MSI NVidia P317). The sound card – sound chip, really – and the Ethernet card are integrated onto the motherboard.

All during the installation, my husband used his digital camera to take pictures of each component and of the process. In addition, for my own file, I made notes of all the model numbers and serial numbers.

- **Document, document, document! You'll be glad you did when a tech support person you're talking to on the phone about your misbehaving computer asks you for the serial number on your hard drive. You'll have the information right in front of you, either in a paper file or in a photograph, and won't have to open up the case and bend yourself into a pretzel to get the serial number off the hard drive!**

Meanwhile, back at the installation procedure, when my husband installed the motherboard into the case and tried to hook it up to the power supply, we hit a snag.

- **Understand that the connector on one part which is supposed to connect to another part may not match up and may need an adapter.**

In my case – you'll forgive the pun – the power supply connector was 20-pin and the motherboard's corresponding connector had 24 pins. No panic yet – there was an adapter in with the motherboard. But when my husband tried to hook it up at the power-supply end, the connector wouldn't connect. It was mis-manufactured.

- **Understand that there are going to be snags and that you just have to accept them when they happen, and come up with solutions. Cussing is optional.**
- **Understand that nature always sides with the hidden flaw.**

We live in a rural area, outside of an unincorporated little town in Florida. The nearest city is Jacksonville, up in the next county. It's quite a ways – especially at these gas prices – to go into the city for our needs. We try to avoid it as much as we can. However, there was not another adapter of the type we needed nearby.

The next day, Sunday, my husband and I made a 60-mile round trip into Jacksonville to CompUSA for another adapter. He had been told on the telephone that morning that they had 20 of the item in stock. Fine. We got there, carrying with us the faulty adapter and the case's original 350-watt power supply as a test bed, since it had the same type of connection. Which leads me to:

- **Be prepared. If you need to go to the store to replace a faulty component, take the bad one with you! Don't try to remember what type, brand, number or placement of pins... you never will. And telephone ahead, and make sure you talk to someone who knows what he's talking about, or should!**

We looked all over the store, ending up at a rack right beside a help station. A young woman came to the counter. We asked her about the adapter. Her first answer was the wrong one: "We don't have those." I informed her curtly we had

been told over the phone they had 20 of that item in stock. She then gave some lame routine about not having been there long and something about some boxes just having come in. She looked to her left, at the rack where we ended up, and said, pointing, "There they are, right there."

- **Do not take nonsense from store personnel. Speak plainly and to the point. Go to the next level, if you have to, repeating that subroutine as many times as necessary, until you get satisfaction.**

We wanted to open the package and see if the adapter therein would fit the power supply. We didn't mind making one 60-mile round trip, but would have been angry to get the new adapter home and find it also didn't fit! The young woman said we'd have to pay for it first, then take it to Customer Service and talk to them about opening and testing it. Thence we went. Two young men confirmed what we'd been told, then gave us a look that said, "Okay, go away." Not me. I took out my money, plunked it down on the counter, and said, "There's my green." I took the receipt, and then we opened the package, took out the adapter, and tried it. It fit.

- **Always ask for what you want. Be firm, even adamant, about it.**

I could have ordered another of the adapters from Newegg.com, I'm sure. But there would have been several days' wait, and I wasn't willing to do that when we could find one near and in a short time. The thing only cost \$7, and I probably would have paid that much just in shipping!

- **Be willing to shell out a little bit more to get what you want when you want it.**

Back home, the assembly proceeded: hard drive (Western Digital Caviar RE 160Gb), DVD-RW (LiteOn SHW-160P6S), DVD/CD-ROM (LiteOn SOHD-6P9SV), card reader (Arrow Micro AICR-01), and the old 3.5" floppy drive from my old computer. He set it all up with the monitor (Samsung Sync-Master 740N: I had to treat myself to a flat-panel monitor), the keyboard (LiteOn SK-1688U), and the mouse (Radio Shack optical mouse 26-592, which I already had), and tested it. It all worked! I had followed all of my husband's recommendations except for one.

- **Even if someone who knows more than you makes recommendations, check them out and see what you think.**

When making my hardware selections, I had gone online to Newegg.com and read the reviews and specifications for the components my husband had picked out. I agreed with all except one: the keyboard. The keyboard he selected was criticized in user reviews for sticking keys (which was why I had trashed my old keyboard) and for having too short a cord. I need a longer cord in my setup, so I selected another keyboard, which I'm happy with.

We set up the machine at my desk. We looked at the BIOS and set it up the way I wanted it, which didn't involve many changes. Then it was time to install Windows XP professional (SP2). It seemed to go well, by all appearances, but we know how deceptive that can be! And it wasn't long until we found out we'd hit another snag. Somehow the OS had set itself up to think the C: drive was a removable drive which had no disk in it, and it wanted to call the hard drive "local drive I:." That would not have worked with some software which insists it be placed on Drive C:. This snag also caused the persistent appearance of an error message telling me that there wasn't a disk present in C: when I knew there jolly well was.

- **Murphy loves operating systems! Whatever can go wrong, will.**

Here I will make a long story short: we used a software program my husband has (Darik's Boot and Nuke) to wipe the hard drive and start all over again. It took two more tries installing Windows XP Professional before the stupid software decided to give the drives their proper names.

- **Be patient, persistent, and courageous when installing software, especially the operating system. It is going to fail a few times before**

succeeding, trust me!

The computer works well, all things considered. I am not able to play a couple of my games, for evidently they require Intel rather than AMD chips. I haven't yet, but I'll go to the respective websites and see if there are any patches for us orphaned AMD users!

- **No matter how well the installation goes, no matter how well the computer is working, there will still be problems. They're inevitable; get used to it or go back to the mid 20th century!**

The important thing is that it will run my genealogy software (The Master Genealogist), word processor (OpenOffice.org), e-mail program (Pegasus), and browser (Firefox), and other things vital to me. As well, it will run some of my games, so I'm happy with that.

- **Once you get it going – enjoy it!**

Karen Rhodes is not a techie, but she does appreciate a well-put-together computer. She's had many careers, some of them quite brief, and is currently studying genealogy through the distance learning facilities of the University of Toronto. She lives in Florida with her husband, her younger daughter, and a calico cat named Tiger.

There is no restriction against any non-profit group using this article as long as it is kept in context with proper credit given the author. The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.

---ooOoo---

CAPTCHA

**(Completely Automated Public Turing test
to tell Computers and Humans Apart)**

Sandy Berger

*From the October 2006 issue of PC News, the journal of
the 1960 PC Users Group of Spring, TX*

Have you ever tried to sign up for a message board or Web service and been presented with an image with letters and numbers which you are asked to read and type into the Web form? While the shape, size, and background of the image varies it always has contains a series of letters and numbers, usually on a graphic background. Often the letters and numbers are distorted and you have to struggle to recognize them, making you wonder why the website is making you go through this extra step. Don't blame the website. This image-recognition routine is something caused by cousins of the nasty spammers who have permeated our email.

The mechanism that makes you type in this information is called a CAPTCHA. If you know what those letters stand for, you will have a pretty good idea of why this mechanism is being employed. CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart.

Here's the story: Spammers have completely infiltrated the world of the Internet. In email they try to get you to buy their wares. On message boards they list links to their Viagra and pornographic websites so that they get better positioning

in the search engines. They overload online opinion polls and they sign up for free email accounts which they use to send out more spam. For the most part, all of this spam activity is done automatically. The spammers send out what we call "bots". These are actually software programs that search the Internet and imitate the behavior of a human. These bots are smart enough to fill out registration forms and so they can automatically register at a variety of websites. We recently had an attack of these automated bots on our Compu-KISS message boards. After years of being unaffected, we suddenly had hundreds of postings that told off-color jokes and [pointed] to pornographic and drug-selling websites. We moved the website to a new area (www.happycomputing.com), but were still inundated by these automated posting. So we installed a CAPTCHA. Now when a new person registers for the message board they must type in the five letters and numbers that they see on the screen to prove that they are human. Since the CAPTCHA is a graphic image, most of the bots cannot read the text like humans can.

The CAPTCHA that we use has letters and numbers that are undistorted, so it is easy to use. If, however, we are attacked by some of the smarter bots that are out there, we will have to distort the letters and numbers slightly to make it even harder for the bots to register. Although a slight inconvenience to the average user, the CAPTCHA is a real roadblock to vision impaired Internet users who use screen readers which, like the bots, are unable to read the text on the CAPTCHA.

It is extremely unfortunate that we all have to be inconvenienced because of the activities of Internet spammers. I really hated to have to install this software, but I had no other choice. The same is true of many other websites and Web services. So when you encounter a CAPTCHA, don't blame the website, blame the spammers!

The Compu-KISS Message Boards can be accessed at www.compukiss.com or directly at www.happycomputing.com.

Sandy Berger, The Compu-KISS® Lady...nationally respected computer authority, journalist, media guest, speaker, and author is a seasoned 30-year computer expert. Sandy is a consumer advocate promoting simplicity, ease-of-use, and stability in consumer technology products. She works with hardware and software developers to help them make their products more user-friendly.

There is no restriction against any non-profit group using this article as long as it is kept in context with proper credit given the author. The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.

---ooOoo---

On page 3 you can see the bus built in 1914 by George Schlitz, a Brooklyn stable-owner. The bus is a trailer pulled by a three-wheeled tractor. It held 120!

The New York Times Store is offering framed copies. If you want one, try:

<http://www.nytimes.com/ProdDetail.aspx?prodId=6486>

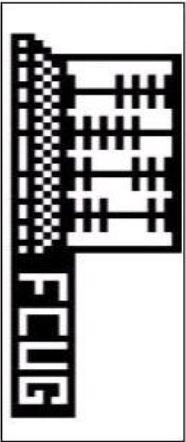
THE VOICE OF FCUG

Journal of the Fairfield County Computer Users' Group

BOARD MEMBERS

PRESIDENT Dick Booth
 VICE PRESIDENT Lenny Bloom
 SECRETARY Bea Mull
 TREASURER Ed Congleton
 MEMBER AT LARGE Charles Bryk
 .NOVICE CHAIRMAN Andy Burns
 Q&A CHAIRMAN Bill Ziemann
 MEMBERSHIP CHAIRMAN ynn Bloom
 REFRESHMENT CHAIRMAN Jane Wiese
 PUBLICITY John Sponza
 CTPC LIAISON CHAIRMAN Jim Sullivan
 VOICE EDITOR Bill Hart
 WEB PAGE - www.fcug.org Mike Brotherton

* Ask Alan HOTLINE (7-10PM) 203-866-7883 *



The VOICE of FCUG

% 280 Main Street
 Westport, CT 06880

First Class Mail

To:

The VOICE OF FCUG is a publication of the Fairfield County Computer Users' Group, Inc. Permission to reprint is granted for non-commercial and non-profit users. Credit is appreciated. Newsletter prepared using OpenOffice 2.0.4 under SuSE Linux 10.1 on a 2.4GHz Celeron 32-bit computer and printed by:

Paul's Prosperous Printing, Wilton, CT 06897
 Telephone: 203-834-1962