Computer Law

Hey Buddy, Can You spare a Dollar?

I want to find out if the Spurs Won

by Bill Wood
Alamo PC Organization, Inc.

I've taken a little liberty with the old saying. But, if Congress passes The Database and Collections of Information Misappropriation Act, H.R 3261, it might not be too far off.

This is one bill that should be watched. It was introduced last October but you have time to contact your Senator or Representative to express your opinion.

The database bill has the potential to be one of the most far-reaching laws in its potential to affect American business. Proponents of the law, such as the owners of the LexisNexus data service and the owner of the Westlaw legal publishing company, say it is needed to cure what they see as a shortcoming of the Copyright Act because you can't copyright facts. Copyright protection only protects the original expression of a fact or thought. Anyone is free to copy and use, even sell, the underlying data. What they can't do is steal your expression of the facts. News.Com indicates that an equally strong lobby has opposed passage of the bill, including the US Chamber of Commerce. (Tech Firms Fail to Squelch Database Bill on Jan. 21, 2004.) Confusing the situation is votes in two different House Committees of different versions of the bill. (Weaker Database Bill Gets House Committee Vote on March 3, 2004.)

Even if it takes significant amounts of time or money or both to assemble and publish the facts, the Copyright act will not protect that investment. Further, the Supreme Court has ruled that merely arranging facts in relatively obvious structures is not enough to satisfy the "originality" requirements of the Copyright act.

So, if you own a business and want to collect and use data for a competitive advantage in commerce, what can you do? Well, for one you can lobby Congress to pass a law that creates a new type of liability. In this case, they are not amending the Copyright law, but rather, they are taking a different track. In that way at least, it is similar to the adoption of the Digital Millennium Copyright Act that made it a crime to distribute a program that circumvents the encryption scheme used to protect intellectual property. You may have every right to make a backup copy of a legally obtained DVD under the Copyright act and still commit a crime. Merely making the copy by disabling the protection software violates the DMCA that has been so much in the news.

HR 3261, as originally introduced by Representative Howard Coble and co-sponsored by Rep. Lamar Smith from our area, would outlaw making available in commerce to others a quantitatively substantial part of the information in a database generated, gathered, or maintained by another person, knowing that such making available in commerce is without the authorization of that person if...

1. The database was generated, gathered, or maintained through a substantial expenditure of financial resources or time
2. The unauthorized making available in commerce occurs in a time sensitive manner and inflicts injury on the database or a product or service offering access to multiple databases
3. The ability of other parties to free ride on the efforts of the plaintiff would so reduce the incentives to produce the product or service that its existence or quality would be substantially threatened.

I had heard for years that some sporting events were trying to monopolize the reporting of the scores. That way, they could sell the rights to report the statistics during the match and maybe even the final scores. At present those rights would be worthless because, any other news media, or person for that matter, could simply copy the facts.

There are many things about the proposed bill that are not clear. On one hand there is a poorly worded exemption that protects news reporting. On the other hand, that exemption may be further limited if the facts are time sensitive. Does that mean that you can't get the Spurs' scores for a day, a week or ever unless you buy a special license to view the standings? Hopefully, the bill will be refined before it is adopted to make it clear how much can be used and how long "time sensitive" information is protected. It may be entirely fair if the monopoly only lasts for an hour or so. It would be completely different if we didn't know the results for a month.

Other key portions of the bill as first introduced rely upon phrases that are not adequately defined. Actually, it is one of the best examples of legal mumbo-jumbo I've seen in almost twenty-five years of practice. What does the phrase "substantial number of members of the public" mean? How would a proposed use be judged if the law directs that "the court shall consider the temporal value of the information in the database, within the context of the industry sector involved?" As stated above, the special treatment for news organizations is not any clearer when it provides,

> Nothing in this Act shall restrict any person from making available in commerce information for the primary purpose of news reporting, including news and sports gathering, dissemination, and comment, unless the information is time sensitive and has been gathered by a news reporting entity, and making available in commerce the information is part of a consistent pattern engaged in for the purpose of direct competition.

If you understand what that really means, please e-mail me with the explanation.

From the April issue of PC Alamode, *newsletter of the Alamo PC Organization, Inc. San Antonio, TX. Bill Wood is an Assistant City Attorney, in the San Antonio City Attorney's Office. He practices real estate and technology law for the city.*

Media Notes

by Bill Petitt
Southeast Virginia Computer Group

Lots of stuff about SPAM, Spyware, Phishing, and robotic email address responders in this month's column. Bear with me as you read through the piece and you will learn some things that you probably didn't know before. You

CAN do something about the problem but it does require action on your part.

Spyware Runs Rampant, Study Says - Many PCs also contain Trojans or system monitoring apps, Earthlink finds.

There's an average of almost 28 spyware programs running on each computer. More serious, Trojan horse or system monitoring programs were found on more than 30 percent of all systems scanned, raising fears of identity theft.

The report presents the results of scans of over 1 million Internet-connected computers. Many of the 29 million spyware programs that were found were harmless "adware" programs that display advertising banners or track Web surfing behaviors. However, the companies also found more than 300,000 instances of programs that are capable of stealing personal information or providing unauthorized access to computers, the companies say.

Tracking Tools

Spyware is a generic term that describes a wide range of programs that track user behavior on a computer, often for marketing purposes. The programs are sometimes bundled with other software, such as peer-to-peer file sharing programs, and installed legally on users' systems. However, once installed, they run surreptitiously in the background and can be difficult to detect and remove. The report covers the first three months of 2004 and compiles information from scans conducted by both EarthLink and Webroot. It is the first of what will be regular updates that track the prevalence of spyware, the companies say.

The results show the proliferation of spyware and should encourage computer users to take steps to protect themselves from spyware, according to a joint statement from both companies. In particular, the detection of over 184,000 Trojan horse programs on the systems scanned and a similar number of system monitoring programs, such as key-logging software, underscore the potential for identity theft and system compromise for Internet users, says a statement attributed to Matt Cobb, EarthLink vice president of core applications.

Protection Available

The Atlanta-based ISP began offering spyware protection for customers in October. EarthLink added a program called Spyware Blocker for free as part of its TotalAccess package of software programs and tools, which EarthLink subscribers can download from the company's Web site. Spyware is gaining greater attention from software companies as well as lawmakers. In recent months, antivirus companies, including Network Associates, have released anti- spyware products. Also, in February, a group of U.S. senators introduced the Software Principles Yielding Better Levels of Consumer Knowledge (SPYBLOCK) Act, which would prohibit installing software on somebody else's computer without notice and consent and outlaw the use of "any information collection, advertising, distributed computing, or settings modification feature" that's installed without consent of the computer's owner.

EarthLink Readies Anti-Phishing Tool — ScamBlocker is designed to track, block access to known swindle sites.

The e-mail appeared to be from a leading retail bank; clicking the link took users to the authentic home page — but a pop-up window led to a site registered in Moscow that sought their account numbers and PINs. It was a "phisher" scheme, and as such scams become increasingly common, ISP EarthLink is readying a free anti-phishing application designed to protect computer users from such cybercrime. EarthLink has released ScamBlocker, a free application available to everyone--not only EarthLink customers--designed to keep Web surfers from accessing the sites phishers use to steal data.

The ISP's timing is good; such attacks are rising 50 percent each month, says the Anti- Phishing Working Group, an industry organization composed primarily of security technology vendors, which has launched an education campaign. The Federal Trade Commission calls identity theft a leading cybercrime. In the case of the faux bank message, users naive enough to provide their personal information could find their bank accounts drained, their credit ratings ruined, or their identities stolen.

Scam Another Day

In practice, ScamBlocker is appealingly simple. The program installs inside Internet Explorer 5.x as part of EarthLink's browser toolbar (which also includes a pop-up blocker and spyware detector), and it automatically downloads a list of known phisher sites. When surfers try to access a fraudulent site, ScamBlocker redirects them to an alerts page on EarthLink's servers. Users can proceed to the scam site or report it to the ISP's abuse team, which tries to get the site's host to shut it down.

But such a service is only as good as its scammer blocklist. Besides its own list of phisher sites, EarthLink pulls information from Net auction giant eBay (a popular target of phisher scams) and antispam vendor Brightmail, which unveiled an enterprise-level fraud-prevention service last December.

EarthLink is in talks with financial institutions and other common victims of phisher "brand-spoofing," but declines to name any of them, says Scott Mecredy, EarthLink senior product manager.

Also, EarthLink plans to refresh its blocklist several times daily, similar to the way antivirus applications update their viral signature databases, Mecredy says. Even so, the first users to encounter a phisher attack may still be vulnerable, says Mark Bruno, Brightmail enterprise product manager. "As with spam or viruses, people at the front end of the curve will still be attacked," Bruno says. "But we can prevent the majority of people from getting scammed."

From Russia With Love

Shutting down the scammers will pose a bigger challenge. EarthLink recently sued spammers also suspected of phishing. But the Anti-Phishing Working Group estimates up to 70 percent of phishers operate out of Eastern Europe, making them hard to pursue, let alone prosecute.

While EarthLink's approach is "fairly promising, these guys are limited in the volume of messages they see," says Dan Maier, an Anti-Phishing Working Group spokesperson. "How well is the eBay /EarthLink toolbar going to stop Citibank scams?"

Maier says combating phishers requires a combination of technologies, including ways to distinguish authentic Web sites from their copycats, heuristic methods to identify scams as phisher techniques evolve, and a global system to share information about attacks in real time. "In the longer run, we're trying to engage Microsoft and other vendors to build [anti-phisher technology] into their products," Maier says.

For the short term, however, he says phisher scams "are a pretty easy way to make money right now."

Security Firm Warns of Spam That Spies

Some e-mail is 'bugged' to alert senders when messages are opened, researchers say.

Hidden code in e-mail messages is increasingly being used to track the success of spam campaigns, according to a warning by an antispam technology company. Up to 50 percent of all spam released in the last year is bugged with so-called spam beacons that send a coded message back to the spammer whenever a spam message is opened, says MX Logic of Denver. Such tracking helps spammers refine their distribution lists and weed out bad e-mail addresses from good ones. The beacons, also known as Web bugs, are created with HTML code embedded in the e-mail. For example, the beacon may be a URL for an image file that is stored on a server controlled by the spammer. When the e-mail message is opened, the e-mail application requests the image and sends along an encoded e-mail address of the recipient. The spammer's server responds by sending the image file to be displayed, but it also captures the e-mail address that was sent in a database of "good" addresses, says Richard Smith, an independent computer security consultant.

Analysis Cited

MX Logic analyzed millions of spam messages that it processes for its 1500 customers each day to study the spam beacon problem, says Scott Chasin, MX Logic's chief technology officer. MX Logic's products use heuristic analysis to spot and block messages containing spam beacons, he says.

The company says renewed awareness of the spam beacon problem is needed because most e-mail users don't realize that they are being tracked by spammers. Also, many e-mail providers are not interested in stopping a "feedback loop" that lets spammers improve their art. MX Logic found that spammers are becoming more sophisticated in hiding the spam beacons from antispam filters. Also, the spammers use the data reported by the beacons to groom their messages and evade detection, Chasin says. The databases that collect the beacon data are often hosted on compromised "zombie" machines, making it difficult to track the spammer responsible for a particular campaign, he says.

Some Protection

Other experts downplay the danger posed by the spam beacons. Microsoft's latest e-mail client, Outlook 2003, automatically blocks the beacons, as do the company's Hotmail Web- based e-mail service and America Online's e-mail, says consultant Smith.

In time, improvements in e-mail client technology and actions by e-mail providers will choke off the spam beacon problem, he adds.

"I think you'll see the 'open' rates drop off altogether, or very dramatically, and spammers will start to wonder 'what are we measuring here?'" Smith says. Others doubt that spammers are really interested in tracking the success of their e-mail campaigns.

"I've never seen much evidence that spammers care about deliverability," says John Levine of the Internet Research Task Force's Anti-Spam Research Group. "I believe that [spammers] have the Web bugs. I don't really know what they'd do with the collected data."

Looking for Lindows? Try Linspire — Lindows, bowing to legal pressure from Microsoft, has renamed its operating system.

The company announced in mid-April that its Linux operating system will now be called Linspire and that a similarly named Web site will be the primary online destination for consumers who want to purchase the company's products or who need support for previously purchased software.

The name change had been expected, following recent court rulings in Europe. The company last week acknowledged that lawsuits by Microsoft challenging the Lindows name would force it to adopt a new moniker for Europe and other foreign markets.

But in the United States, where Lindows has had more interim success in its legal battles with Microsoft, the name Lindows will still be used in certain instances and as the corporate name.

"Despite our victories in the United States and overseas, a name change is still necessary to counter Microsoft's strategy to sue us in courts around the world. We're hoping that this puts a halt on the international lawsuits," Michael Robertson, CEO of Lindows, said in a statement.

The San Diego-based company is locked in a 2-year-old legal battle with Microsoft, which says that the Lindows name is an infringement of its trademark for the Windows operating system. Lindows argues that the trademark is invalid, because "windows" is a generic computing term.

The U.S. case, already delayed several times, is likely to go to trial later this year. The judge overseeing that case has denied Microsoft's requests for an injunction that would bar Lindows from using the name. But the software giant has been more successful overseas, where judges in Finland, Sweden and the Netherlands all have granted such injunctions.

Linspire is similar in features and capabilities to the original open-source Lindows operating system and customers will not need to upgrade, the company said. All Lindows software products will carry the Linspire brand within two weeks, it said.

As of Wednesday, the Lindows.com site carries a prominent notice that "pending Lindows' appeal, visitors from the Netherlands, Belgium, and Luxembourg are not permitted to access the Lindows.com website or purchase Lindows products." The identical Linspire site carries the same message.

Stampede for patches disrupts Microsoft update site - The crush of millions of Windows users trying to patch their computers overwhelmed Microsoft's update service for several hours after new security fixes were made available, the software giant acknowledged on Wednesday.

Immediately after April 13's release of four patches that fixed a score of flaws in the company's operating system, traffic to Microsoft's Windows Update site spiked higher than seen during any previous update, reaching a sustained download rate of more then 50GB per second. Past patches have resulted in 2 million people visiting Microsoft's Windows Update site every hour to download fixes. This time, between 3 million and 4 million users came to the site. As a result, many customers found that the scan didn't work properly and they were not able to download the latest patches.

"When the patches went out yesterday there was a significant wave," said Todd Weeks, director of operations for Microsoft.com. The increase led to delays for users who wanted to immediately download the latest patches from the service. "After about the first four hours, it was essentially resolved." By that afternoon, the company had about doubled the ability of the servers to handle requests by adding more servers that had better processors, Weeks said. By the next morning, the software giant's update servers were handling 4 million visitors every hour with no issues, he said.

The events present the latest problem for Microsoft as it continues its two-year-old Trustworthy Computing initiative. Although the software giant has taken major steps to alleviate security concerns, such as delaying its next version of Windows in order to divert developers to its Windows XP Service Pack 2 security update, Microsoft has also had to contend with releases of critical patches to deal with large virus epidemics among customers.

Nonprofit group Pathfinder International encountered delays in updating its Microsoft computers the next day, said Kevin Greene, senior network administrator for the group. Pathfinder has servers in the United States, Peru, Brazil, Bolivia, Bangladesh, Egypt, Ethiopia, India, Kenya, Nigeria, Vietnam, Pakistan, Yemen, Tanzania and Uganda. After one of those computers had been infected by the MSBlast worm last August, the group focused on applying patches as soon as possible.

"Microsoft's decision to release updates to 90 percent of the computers on the planet on the same day, coupled with its announced desire for us to all update on the same day, places a considerable burden on Microsoft to ensure it has the bandwidth, equipment and other infrastructure necessary to ensure that we can do that efficiently," Greene said. "My experience this morning, and in the last round of updates in February, indicates that the infrastructure is lacking."

Internet performance measurement service Netcraft noted the problems as well, stating: "A browser request through Internet Explorer eventually raises the site after an extended wait, and in some cases it is possible to successfully download and install updates over a broadband connection."

The flood of users led Microsoft to add the ability to regulate the rate at which Windows Update will try to download patches from the company's servers, Weeks said. The new feature will act as a spigot on the electronic data, evening out the demand for downloads.

The current problems were solved by throwing more computing power at the issue, said Stephen Toulouse, Microsoft's security program manager. He added that--on the positive side--the flood of users means more customers are worrying about security.

"People are now just waiting to get the update," he said. "We are pleased (that customers are more aware). We will do whatever it takes to provide these updates to our customers as demand increases."

Security issues move Linksys routers off your short list

Following is a story told to me by a friend:

In many cases, households have more than one Internet user and are installing turnkey connection-sharing appliances. The two companies that most often come to mind for him as providers of these appliances are the recently Cisco-acquired Linksys and the as-of-yet-to-be acquired NetGear. Linksys is apparently having some engineering difficulties that are leaving its customers exposed to potential security problems.

There is a new and looming threat to all Internet users — the mini Distributed Denial of Service attack (mDDoS) — my friend's four-year-old Linksys BEFSR11 cable modem router/firewall was having security issues that couldn't be solved by upgrading its firmware with the most recent download from Linksys' Web site. To address the router's shortcomings, Linksys suggested that he try a newer router. Although the one they sent him — a four-port BEFSX41 — had more robust logging capabilities (your ISP may refuse to do anything about a DDoS attack unless you can produce a detailed, e-mailable log), he had difficulty getting it to work securely and reliably. His troubleshooting attempts reminded me of some problems I had with the older BEFSR11 two years earlier, after I had upgraded its firmware in order to get support for Universal Plug- n-Play (UPnP).

One of the advantages of UPnP is that, instead of leaving certain ports on your firewall permanently open to support certain applications, UPnP-capable applications running inside a network (like instant messaging applications) can make a request to open the ports temporarily. This is supposed to improve the security of your firewall because, as long as certain applications aren't in use, the ports that they typically rely on stay closed. Also, those applications don't have to always use the same port. The resulting lack of predictability means that hackers face a lot more trial and error testing before they can successfully leverage any open ports. However, the minute I activated UPnP on my old router, MSN messaging broke and my network connection kept going up and down until I went into the router's administration console and disabled UPnP altogether.

Between the UPnP problems with the old router and key mDDoS vulnerabilities that haven't gone away with the new one, and some other reliability problems he was having with the new one, I'm beginning to wonder how well Linksys is testing its routers and firmware upgrades before releasing them to the public.

For starters, as Gibson Research's ShieldsUp firewall vulnerability test will show, most Linksys routers leave port 113 closed by default. Firewall ports have three modes: open, closed, and stealth. The stealth mode hides a port's existence altogether (if all ports are stealthed, the existence of the entire Internet connection is basically hidden), while a closed port will actually acknowledge queries from the Internet by saying "Yes, I'm here!" A well-executed mDDoS attack, such as the one that hit my friend's Linksys router, will send the router/firewall into such a query-acknow-ledgement frenzy that the device quickly becomes too overwhelmed to handle any legitimate traffic. To users relying on that connection, the connection appears to be down. So vulnerable to such attacks are router/firewalls with any port open or closed that Gibson's ShieldsUp test will give a clean bill of security health only to a firewall/router with all of its ports stealthed.

According to a Linksys spokesperson, "Our engineers used to have this port stealthed, until we started getting a lot of complaints about using IRC. The solution was to keep it closed at the time." In subsequent e-mails, Linksys said that it was "still under discussion on how to implement [a fix]. This will impact all of our product line, so we need to carefully plan for it." Let me repeat that: "All of Linksys' product line" is affected by this vulnerability. So, is Linksys' rationale for leaving port 113 closed instead of stealthed justified?

According to Gibson Research president Steve Gibson, the answer is no. "Port 113 is known as the IDENT port," said Gibson. "When a user connects to an IRC server, that server turns around and makes an IDENT query back to the user's system. If the user's system is running an IDENT server and port 113 is open, their system will respond to the IRC server's query with information like the user's name and maybe their phone number. If port 113 is closed, the IRC server would at the very least get an acknowledgment, telling it that someone is there. If port 113 is stealthed, the IRC server won't even receive an acknowledgment and, on the assumption that no one is there, will think the connection attempt is bogus and deny the connection. But that practice, which dates back to the early 90's, has long since stopped. If you really tried, you could probably find an IRC server on the Internet that still does IDENT queries, but no one really does it anymore."

Gibson went on to describe how easy the fix would be. "The way ZoneAlarm dealt with this is that it would keep port 113 stealthed, and if it detected that an IRC client was having difficulty achieving a connection, it would dynamically switch the port's status and allow only a connection with that IRC server," said Gibson. "Nothing prevents Linksys or any other router/firewall vendor from programming the same sort of capability into their devices." What firewall/router does Gibson use? "I've already switched from Linksys. Now, I use NetGear."

Whereas Linksys is, in my estimation, making the ill-founded decision to leave port 113 closed instead of stealthed in order to support a hardly used legacy technology, its closest competitor, NetGear, has port 113 stealthed by default on its devices.

Linksys, Boingo Boost Hotspots — New small business router eases setup to encourage spread of Wi-Fi networks.

Small businesses can now turn on Wi-Fi hotspots to compete with better-known rivals without the hassle of setting up the whole service themselves, according to Cisco Systems' Linksys division and Boingo Wireless, which have teamed to market Hot Spot in a Box. The feature is available immediately in the United States on the Linksys Wireless-G VPN Broadband Router. Once the router is set up on a broadband connection, the business can join the Boingo Roaming System. Then, Boingo subscribers can use the hotspot just as they would any other Boingo hotspot. Non-subscribers can sign up for a day's service or subscribe to Boingo on-site.

The router is available now for an estimated street price of $230. Boingo, along with carrier partners that include WorldCom, EarthLink, Fiberlink Communications, and Infonet Services, operates about 7000 hotspots worldwide. This offer is aimed at businesses such as doctors' offices, retail outlets, and office lobbies as well as coffee shops and restaurants, according to Boingo.

How It Works

Wi-Fi hotspots have proliferated in locations frequented by business travelers, but before the technology catches on with the general public it will have to become "an order of magnitude more pervasive," says Christian Gunning, director of product management at Boingo, in Santa Monica, California. "We think this is the type of product that starts to generate that kind of availability... but it's a multiyear proposition," he says.

The small business buys the device and the broadband connection but gets administration support and marketing for free. It also gets paid every time a customer uses the hotspot. The business gets $4 of the $7.95 fee for a day's subscription, earns a one-time $20 "bounty" when a user buys a Boingo subscription at the site, and gets $1 from Boingo every time a subscriber walks in and logs on.

Billing and back-office services are handled by Boingo and its service provider partners. Small businesses can turn to Boingo's Hot Spot in a Box administration site to make configuration changes or monitor their traffic.

Businesses with existing Wireless-G VPN Broadband Routers can download the Hot Spot in a Box firmware free from Linksys's Web site, the companies say. The system allows businesses to use the wireless LAN for their own purposes free of charge while offering the public paid access, with a firewall between the two to secure business information, Gunning adds.

Are Hot Spots Safe?

You and your notebook are at a corner café, wirelessly surfing the Internet. You buy a book from Amazon.com using your credit card and check your savings account balance at your bank's Web site. It's all very cool, in a new-millennium sort of way.

But is it secure? Wireless networks broadcast data over radio waves, and anything transmitted over the airwaves can be intercepted. That's why wireless networks are inherently less secure than wired networks.

By definition, public wireless networks are designed to be accessed by anyone within the Wi-Fi hot spot's broadcast range, usually up to 150 feet from an antenna. Because these wireless networks are open to all (either for free or for a fee), it's possible that sophisticated hackers could grab your data out of the air, decode it, and use it, according to C. Brian Grimm, marketing director of the Wi-Fi Alliance, a nonprofit association.

This doesn't mean, however, that you have essentially recited your credit card and bank account numbers aloud for everyone in the café to jot down. While no security system is infallible, there are strong security precautions in place to protect wireless network users.

Look for the Lock

When you bank or shop online, your transactions are usually handled on secure servers that use Secure Sockets Layer, an encryption protocol that creates a secure Internet connection between the client (you) and the e-commerce site's server.

Web retailers that support SSL — and the vast majority do — direct your transactions to areas of their site that have URLs beginning with "https" instead of the standard "http." This indicates that the area of the site you're in is secured by the SSL protocol. Also, you'll notice a lock icon displayed in the lower right corner of the Web browser window, which indicates the area of the Web site you're in is secure.

For example, let's say you're going to shop for a book at Amazon.com. You won't notice the "https" or the lock icon in your Web browser while you're browsing for books, because that activity doesn't need to be secure.

But once you begin the checkout process, in which you're required to enter your credit card information, you're directed to a secure Amazon.com server. At this point, you'll notice that the Amazon.com URL in the address line of your browser now starts with "https" instead of "http," and there is a lock icon visible in the bottom right corner of your browser window.

Virtual Private Networks

Other security precautions are also available to protect wireless network users. Many companies, particularly large enterprises, offer their employees Virtual Private Network connections to the company's network and the Internet. VPNs use encryption and other security methods to give wireless network users the same kind of privacy that wired networks typically have.

Some wireless network service providers also offer VPN security. For example, EarthLink Wireless High Speed, which the Internet service provider EarthLink offers in conjunction with Wi-Fi hot spot provider Boingo, includes built-in VPN security, according to EarthLink. The service is offered at some 2500 locations such as airports, hotels, and coffee shops at rates beginning at $5 per month. For more details, go to: https://store.earthlink.net/cgi-bin/wsisa.dll /store/frameset.html?product=wifi

Is Your Notebook Secure?

Wireless networking has its own security protocols, too. The Wireless Equivalent Privacy protocol has been around for years, but has fallen out of favor because its security is far from airtight.

A newer wireless network security protocol, Wi-Fi Protected Access, started showing up in new products in early 2003. WPA provides encryption and other privacy protections that are far stronger than previous Wi-Fi protocols, says Grimm.

Some notebooks have built-in wireless networking capabilities. So how can you tell if the wireless networking chip in your notebook supports WPA? The Wi-Fi Alliance site maintains a list of WPA-certified products, including internal wireless networking cards found in notebooks and desktops. You can browse by vendor and product type at the Wi-Fi Alliance site: http://www.wi-fi.org/OpenSection/certified _products.asp?TID =2

If your notebook's internal wireless networking card doesn't support WPA, you may be able to upgrade the card's firmware to add WPA support. Check the online support section of your notebook vendor's Web site or the manufacturer of your notebook's wireless network card for updated drivers that support WPA.

External wireless network adapters, such as PC Cards and USB devices, may also have updated drivers that add WPA support. Check the adapter manufacturer's online support for the latest drivers.

If all else fails, you can buy a new, external WPA-compatible wireless network adapter for about $50 or more. You can browse a list of such devices at the Wi-Fi Alliance link listed above. At the site's Certified Product Listing page, in the Filter by Company drop-down menu, select (Show All); in the Filter Products By menu, choose External Card; under Capabilities, click to check Wi-Fi Protected Access; and then click the Submit button. The products listed include links to vendor Web sites.

Keep in mind that Microsoft Windows XP doesn't support WPA, so you'll need to go to the company's support site to download an update: http://support.microsoft.com/?kbid =815485 The Microsoft site includes lots of helpful information about WPA as well.

Extra Protection

Though Windows XP has a built-in firewall that helps prevent unauthorized access to your computer files, you might consider more robust programs such as ZoneAlarm Plus 4 ($40) or ZoneAlarm Pro 4 ($50). Both programs include a feature called Mobile PC Protection, which automatically detects and protects you on the wired or wireless network that you're connecting to. To download ZoneAlarm Plus or Pro, go to the Zone Labs site: http://www.zonelabs.com/store /content /home.jsp

From the May 2004 issue of The Umbella Online, *newsletter of the Hampton Roads Virginia Computing Community.*

The Lazy Webmaster

Copy and Paste Your Way to Fame and Fortune

by Susan Ives

Alamo PC Organization, Inc.

Copying and pasting are the lazy Webmaster's salvation. No, I'm not talking about stealing content. Everything on the Internet is copyrighted because it is saved permanently. If you write a poem or draw a picture and scribble it on a piece of paper, attach it to an e-mail, put in on a Web page or save it on a floppy, it's copyrighted. And so is the other guy's stuff. So don't go grabbing other people's intellectual property.

What I'm talking about is copying- and-pasting to save time and energy.

If your basic Windows skills have atrophied:

* Copy text by highlighting it (drag the mouse across it while clicking the left mouse button) and then pressing Ctrl+C. Or, all Windows programs have a menu bar at the top of the screen — you can select edit-copy.

* Paste text somewhere else — even into another program — by positioning your cursor where you want to drop the text and press Ctrl+V. That V is meant to represent a copy editor's caret, which means insert, but you can think of it as vomiting it back onto the screen if that makes life easier for you. Edit-paste also works.

I've found that some of my students don't realize that they can copy and paste between applications. The copy command places the copied data into RAM, random access memory. It's floating in computer memory, available to use in any program until you copy something else, which writes over it. You can copy something from your browser, for example, and then paste it into your HTML editor.

Yes, you can copy right off of the browser screen! If you want to be mean, you can prevent others from doing this to your site. Just put this line of code in the <BODY> tag:

<BODY ondragstart=”return false” onselectstart= ”return false”>

This is JavaScript, so it won't deter those who turn their scripting off or use browsers that don't support Java. People can also view the page source and get the marked up text.

However, it does make it harder for people to “borrow” your text.

When I am creating links to other sites, I always, always copy and paste the URL from the address box to make sure I get it exactly right. O and 0 look alike. So do l and 1.

Copying and pasting text sometimes creates weird line breaks. If you are copying from e-mail you will get those >>> that indicate quoted text. I use a free utility called “the Cleaner” to get rid of both the line breaks and the >>>. You can download it from ronbrandon.com

You probably know that you can save most graphics from the Internet to your hard drive by right-clicking your mouse on the graphic and then choosing “save picture as.” In Internet Explorer, make sure to add the file extension to the graphic when you save it. If you don’t want people taking your graphics, you can disable the right-click with another JavaScript (put this anywhere on your page):

```
<SCRIPT LANGUAGE=”JavaScript1.1">
<!-- Begin
function stopthief(ie) { var warning = “Right clicking this page is notallowed.”;
if (navigator.appName == ‘Netscape’ && ie.which == 3) {
alert(warning);
return false;
} else
if (navigator.appName == ‘Microsoft Internet Explorer’ && event.button==2) {
alert(warning);
return false;
}
return true;
}
document.onmousedown = stopthief;
// End -->
</SCRIPT>
```

They will get a dialogue box that says, “Right clicking this page is not allowed.” You can see where those words are in the script. Change them to something nastier if you prefer.

Background images, often seamless tiles, can also be copied and saved. Place the cursor somewhere on the background, but not over another image. Right-click your mouse, and from the dropdown menu select “save background as..”

View source:

You do know about view-source, don’t you? This is the best tip I got when I was a new Webmaster. You can look at the source code for just about any HTML document by going to view-page source from the menu bar. This is a useful way of seeing how another Webmaster created a certain effect, or where a script originated, or even, sometimes, what program was used to create the page. You can copy code snippets directly from the source. Copying an entire design would be immoral, if not illegal.

Lorem ipsum:

When designing a site, I work on the structure first, then the colors and design, and add the content last. I do need text as a placeholder, however, to see how a site will look. Since the 16th century, the convention is to use “lorem ipsum,” paragraphs of garbled Latin, as placeholders. It keeps me — and clients — from being distracted by specific words in sample content. I found a handy lorem ipsum generator on the Internet — it will create as much as you want. You can even select a specific word count, so if your content is always 650 or 900 words, you can get exactly that. It’s at lipsum.com.

Copying and pasting is critical to everything I have talked about for the last six months. It’s a minor skill, but one that you will use every day.

Reprinted from the April issue of PC Alamode*, newsletter of the Alamo PC Organization, Inc. San Antonio, TX. Susan Ives is a past-president and past-webmaster of Alamo PC.*

PCI Express: Say Goodbye to AGP and PCI Slots

by Timothy Everingham
TUGNET

Those of you who have been around personal computers for a while might remember plug in cards slots referred to as ISA, EISA, Microchannel, and VESA Local Bus. ISA, EISA, and Microchannel were replaced by PCI. VESA Local bus was primarily for video cards, which was replaced by PCI, then AGP slots. It was a fun time during these card slot transitions because many times you could not use the plug in cards from your old machine in your new computer or motherboard or if you did it could slow down the entire system. Well guess what, its time to do it all over again. Intel has come up with a new slot standard PCI Express, which will start to show up in computers/motherboards this spring.

PCI came out in 1992. Today these slots and its data bus technology are used for things not envisioned when it was under development over 12 years ago. PCI has its limitations and the PCI pro slots never became popular. The limitations are coming to the forefront in delivering multimedia content and Gigabit Ethernet. Of course getting higher frame rates at higher resolution and quality for video games also is an issue. PCI has been evolving over time increasing its speed to five times the original, but it has reached its limits of development. Many say that stretching out the AGP to 8x speed might be pushing at its limit too.

First let us look at the current PCI architecture you will find on most motherboards. The CPU/Microprocessor communicates with the first of two data bridges, normally referred to as the Memory Bridge or Northbridge. The Northbridge not only communicates with the CPU; but also communicates to the AGP port, which is where your main graphics card is (usually the only graphics card). It also communicates with your RAM. The fourth thing it communicates with is the second data bridge, known as the Input/Output (I/O) Bridge or Southbridge. The Southbridge also communicates to your plug in slots/cards, drive controllers, and USB, Fireware /1394, parallel. serial, game, keyboard and mouse ports. The theoretical speed limit of the Southbridge communication to I/O including the PCI slots is 133 MB/second. All of the communications in the system are parallel with none of the data having any priority over any other. Blocks of data have to be sent one at a time and cannot be done concurrently. Therefore the data is transferred from one section of the motherboard to the next section based on the order received, not the importance or whether a piece of data arriving by a certain time to its destination is critical.

PCI Express, instead of using a parallel bus architecture, uses serial networking typology with only two wires for each direction. At higher speeds, it allows concurrent transfer of data while having a similar look and the same type of Northbridge/Southbridge architecture as currently in desktops and laptops.

However, in servers the Southbridge is eliminated producing greater data throughput. The PCI slots initially have a 250 MB/second throughput, but the scalable width technology (increasing the number of wire pairs) enables slots and cards to communicate at 32 times that speed in later implementations using longer slots. But the typology can also use network switching type technology, giving data priority and quality of service functions. Hot plug/swap of components is a native part of the architecture.

The PCI Express Graphics Port, replacing the AGP Port, will have a 4GB/second transfer rate in its initial configuration, double that of the current 8x AGP ports. For laptops units there will be a new plug-in card to replace PCMCIA called ExpressCard. It will come in two forms, one that more looks like a PCMCIA card refereed to at the 34 module form factor (34 x 75 x 5 mm) and a more oversized L looking card called the 54 module form factor (54 x 75 x 5 mm). This new architecture is compatible with existing operating systems. Also the new PCI Express slot is capable of being placed alongside current type PCI slots so a choice can be made which type of card can be used in a motherboard just like was done with ISA slots and current PCI slots. The standard PCI Express slots being put in motherboards this spring (1x) will be a lot shorter than the standard PCI slots.

All of this will mean that a lot of issues having to do with multimedia on desktop and laptop computers will have been solved. It also opens wider use of Gigabit Ethernet on local area networks. It also enables the prospects of new motherboard form factors and computer case designs. As the transition from ISA to PCI was an interesting transition with computer buyers having to do more research and planning on their purchases, the move from PCI to PCI Express will do the same. However, as was with the previous transition, the performance and capability increases of computers will be profound. Further information on PCI Express can be found at www.express-lane.org.

Timothy Everingham is CEO of Timothy Everingham Consulting in Azusa, California. He is also Vice Chair of the Los Angeles Chapter of ACM SIGGRAPHand is also on the Management Information Systems Program Advisory Board of California State University, Fullerton. In addition he is the Vice President of the Windows Media Users' Group of Los Angeles. He is also part-time press in the areas of high technology, computers, video, audio, and entertainment/media and has had articles published throughout the United States and Canada plus Australia, England, & Japan. Further information can be found at <http://home.earthlink .net /~teveringham>

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.

From The DealsGuy

by Bob (The Cheapskate) Click

Greater Orlando Computer Users Group

Because of all the great feedback, I'll start this month off with more about interesting trade shows we have worked, but I'd like to change the topic next month to technology for homes. March began with one of my favorite shows called MegaCon, otherwise known as the "Comic Book" show. I first worked it last year and was warned I would be seeing all those crazies and weirdos. Well, I WAS certainly surprised, but I didn't interpret the attendees that way at all. I saw many people who loved their hobby and had even hand crafted their costumes to represent certain characters, such as comic book, game, space and other characters. Many costumes were absolutely gorgeous. I saw bodies and faces that required much time for makeup to get the necessary effect, and yes, some looked weird (like they are supposed to). I enjoyed the folks with the space suits and those looked pretty awkward to wear. One young woman was a bit too daring with her costume, but she was quickly noticed, escorted from the show and informed that paint does not substitute for wearing an upper garment in public, especially when there are children present. Never mind that the men loved it. We stopped another woman with extremely skimpy lower attire and referred her to show management.

Looking for a badge or wristband on people entering with costumes was not easy, but some held them out or pointed to them for us. The show occupied 108,000 sq. ft. of exhibit space with about a quarter of it devoted to special artistry tables, celebrity autograph tables, game tables and the food area. The rest was vendor booths. There were lots of things other than comic books, including robots and digital badges. This show also used several large meeting rooms off the lobby area that worked with such things as games and animation movies in 3D. They well exceeded the 20,000 expected attendees and the show floor was very packed. There were eight famous celebrities, such as June Lockhart and Angela Cartwright (of Lost In Space fame) signing autographs. We met most of them since they went through our entrance, and they were great people. My grandson took home my show guide so I can't list them all.

I talked to many attendees asking how they acquired their beautiful costumes and most said they had hand crafted it themselves with help from family members. I talked to many people with professional jobs and good incomes that loved this hobby. Even though I had a very intensive job, I was entertained all day long just by watching the people. I saw more daring cleavage during this show than any other I have worked. Remember, a badge or wristband (some won't wear a wristband on the wrist) might actually be looped anywhere so they are difficult to spot. Of all the shows I have worked, this show's attendees were by far the nicest to work with. We were never angrily challenged for trying to enforce the rules and everybody simply asked what they had to do. Mostly, acquiring a proper badge or wristband was the answer. Even though this show was mostly young people, there were some older generation and a few seniors. Since there were three other trade shows in the building at the same time, some tried to use other badges.

We also worked the Home Electronics Expo [http:// www.ehx2004 .com] and [http://www.virtualEHXspring.com] in March and I was impressed with all the amazing technology that can improve your lifestyle (at a price). Most of it was about automated /remote lighting (low voltage), video and sound. All this can be controlled from anywhere in the house that you desire, and even remotely if you prefer. You can dial home (phone or computer) and check your refrigerator (if you're stopping at the store), start the food preparation, have your favorite music going and set the house temperature as well as take a look at the children or pets through a camera. There were lots of wall mounted thin screen TVs in the show, but the largest I saw on display was only a 60" plasma screen (they come as large as 80"). Many vendors specialized in cabling, or switching, only. Others specialized in audio or video specialty installations and a few distributors such as Worthington had booths. There were a multitude of audio speaker designs, including some wall mounted ones that blended in with the decor, but had great sound.

There were also electrically operated driveway gates, garage doors, and even windows that would close automatically, such as by a rain sensor, or by remote control. A couple of booths offered timed or remote controlled drapery rods and vertical blinds. My favorite booth was the one with weather stations. [http://www.peetbros.com] I was devastated when my own weather station went out a year ago, but it was a 20-year-old Heathkit and that company was gone years ago. I need a new one. I liked the design of these because of the illuminated readings rather than LCD, and it so happens their offices are within driving distance for me to check on a deal.

Unfortunately I missed working the Microsoft Show being held at the Gaylord Palms Resort, but we prefer not to work for the company that was given the security job, although they had asked us. Now here is what I have:

Reminder On A Great Software Deals

Colleen Toumayan from Executive Software called to remind us all that their special offer for Diskeeper Professional Edition 8.0 bundled with Undelete Home Edition for just $49.95 is still good. Check at [http://consumer.execsoft.com/home.asp] to order this bargain. We all know what great products Executive Software produces.

We All Like Freebies

Sally Springett, editor for The Rochester Computer Society *Monitor* [http://www.rcsi.org], sent me this URL that I found interesting and felt you might like it also. If you don't like rebates, then skip this and keep going. This URL [http://www.freeafterrebate.info /index.php?topic=Hardware] offers leads to purchasing products that will be free after the rebates. Be aware that third-party vendors offer these products and you should do your own homework diligently before you decide to order. It might even be an older or discontinued product and you will probably pay a shipping charge. With that caveat in mind, check it out and I imagine that it will change quite often.

Help For Your E-mail

I have a couple of friends who use MailWasher and say it works pretty well to eliminate spam, although it stopped a few legitimate e-mails at times. I questioned Hewie Poplock, a good friend whose opinion I value, who has used MailWasher for a two years and he is completely sold. He says if you set it up right, it won't filter out good messages, but if you get too fussy, it could happen. Sounds logical, but I have not had enough experience as yet. It incorporates learning by Bayesian statistics and uses FirstAlert!, a real-time global spam database. Something else I like is that you can check your e-mail right on the server instead of on your own computer, if you prefer.

Mathew Miller, Product Development Manager for MailWasher, made a special offer available for user group people and I asked him to extend the deadline so I could include it in my June column. He agreed so you get the price advantage. Mathew is offering us MailWasher Pro and a one-year subscription to FirstAlert for just $29.95, a saving of $7.00. You will need the promotional code of QTUGAD to order. This offer is good until July 31, 2004. Get more info on this tool for all that disgusting spam and download at [http://www.firetrust.com /products/pro/].

That's it for this month. Meet me here again next month if your editor permits. This column is written to make user group members aware of special offers or freebies I have found or arranged, and my comments should not be interpreted to encourage, or discourage, the purchase of any products, no matter how enthused I might sound. Bob (The Cheapskate) Click [bobclick@mindspring .com]. Visit my Web site at [http://www .dealsguy .com] for interesting articles from user group newsletters. I also posted some interesting *new* website pages for your viewing. Explanation on the Web page.

Your Internet service provider should be able to tell you your best-case speed. But the Internet is like the drive to work: Sometimes it's fast; other times, it makes you grind your teeth. If you want to test your connection, here are a couple of sites:
Bandwidth Place:
http://bandwidthplace.com/speedtest/
Broadband Reports:
http://www.dslreports.com/stest

O'Reilly Needs Your Help

We have yet another book in the wings — this one focusing on home networking annoyances. Everything from cabling hassles to setting up a router to wireless access points to fussing with TCP/IP settings to installing a shared printer. Whether you've set up a wired (Ethernet, phoneline, or powerline) or wireless (802.11a, b, or g) network, merely shared a DSL line, or networked a bunch of PCs and Macs, feel free to share the annoyances you've encountered along the way.

If you or any members of your group have home networking annoyances you'd like to see solved, email marsee@oreilly.com with "Home Networking Annoyances" in the subject line. Please note what hardware, software, and/or service is giving you grief (e.g.: a LinkSys Cable/DSL Router with 4-Port Switch, SMC's EtherPower II network cards, SBC DSL, Windows XP, etc.).
An example:

The Annoyance:

I added a new computer to my network, but it doesn't appear in My Network Places or Network Neighborhood on any of the other computers. The Windows help files tell you to reboot all the other computers on the network in order to see the new computer, but there's got to be a better way!

The Fix:

There is. Assuming your hardware connections are working, and you've created at least one shared resource on the new computer, you don't have to reboot the rest of the network to see the new computer. Wait twelve minutes. Honest. Could I make that up? Get a cup of coffee, empty the dishwasher, or change all the burned out light bulbs in the house. Then open the network folder again, or press F5 to refresh the display if you didn't close the folder. You should now see the new computer.

Why does this happen? The icons in the network folders (My Network Places and Network Neighborhood) are controlled by a service called the Computer Browser Service, which browses the network, peers down the pipes (including the virtual pipes of wireless connections), and checks to see who's on board. In a peer-to-peer network, the computers elect one of their own as a browser master using a complicated scheme that involves a private conversation among the computers (held secretly so you aren't aware of it and can't control or interfere with it). The browser master runs the browser service every twelve minutes, and populates the network folders of all computers on the network with icons representing the computers it finds.

Society News

Program Meeting

May 11, 2004

by Jan Rothfuss

Helps Half Hour

Led by: Bill Statt

Q: New computer with XP Home. HP printer works but, with each boot up, gets the message about 'finding a new piece of hardware.'

A: Try to uninstall printer, restart the machine and let it go through the find/install process again. Do not turn the printer on until after the start up process is finished. Follow the directions: Put the disk in, then load the printer installation process.

Q: Has the sasser worm been found on anyone's computer?

A: Worm is obtained through web access - no need to open an email. Need to install patch from the website. Do not install Service Pack 2 but get the patch. Firewalls will protect you. Problem for Win2K, XP and Win 98.

Q: Mozilla mail program sent a message about getting a virus.

A: Message probably was not sent from your machine but generated by a virus.

Q: Tried to use antivirus program on new XP machine. Could not download/apply

A: May need to install Stinger software. Will need to turn off your system restore functionality as virus will hide there. Then install AVG software.

Q: Does built in firewall in XP prevent infection?

A: No. You need another. Zone Alarm will stop it. Provides security checks for transfer requests from both directions - in and out of your computer. Can use master list of permission files in Zone Alarm and evaluate access again.

Q: Attempting to install service pack 1 but stops.

A: Download more recent version 1.a

Q: What is Data Miner?

A: It is a spyware/tracking program that logs all Internet visits. Then your ads will be customized according to your personal preferences. Best to run Ad-Aware or Spy-Bot that can be run to remove the programs.

Q: Attempting to send out email but getting a message about sending pictures. Outlook Express and WinXP

A: May want to install service pack 2. May have some corruption in your extensions - check out your file associations. Could switch to Outlook or try Mozilla or Eudora. Thunderbird is just email that could be used. Reminded people not to use Internet Explorer as your browser. Allows too many problems to invade your computer.

Q: Uses MSN Messenger, using a camera webcam. When adds the webcam, XP simply restarts.

A: Must be sure to download the XP drivers for the webcam. Be sure to get the newest ones by going to the camera website. Be sure to watch references to the service pack installed as well.

Q: After one month in Florida, using Frontiernet emails, it seems that 1/3 of outgoing mail are not actually going out. Win98 using Outlook Express or Eudora

A: Go to Frontier Webmail website to discover whether mail is really lost. All should be found there or a reason given why it is not being sent. Can use this location to set up or turn off block? Many systems are blocking HTML formats and suspicious attachments.

Business Meeting:

Led by Arpad

Summer Picnic: Perinton Park cabin 4:00 — 10:00 p.m. August 10th is the date. $5.00 deposit fee, returned when you arrive. Sign up to choose your meat and what you'll bring. Salads (A - I), Dessert (J - Q), Munchies R - Z). There will be a flea market — bring donations. Elections will be held next month — still looking for a secretary.

New members: Dr. Clifford Jacobson, Dennis MacMahon, and George Platt.

Renewals: Frank Howden, Robert Panello, Ralph Squire, Irwin Wiener, Claude Fedele, Milo Turner, Jim Murdock, Bernice Blake, and Ron Matteson.

Program Meeting:

Linux install by Max Kessler.

Tony's donated PC is a Pentium II with 128 mg RAM. Began by booting from the Mandrake CD. Install initiated properly. Be sure to record your password. KDE is the desktop software that does look a lot like Windows. "Start" button is called 'Kicker' used to show the options/programs that can be run. Each set of menu choices was walked through with the group hearing descriptions for each optional program. There is a great set of screensavers provided. Recommended that new users refer to a "Linux for Dummies" textbook to become familiar with the new features and programs. Those who currently run Windows will generally feel right at home. Arpad reminded the group that Linux does not support many games properly.

Then we brought up Fedora. Demonstrated that the soundcard and speakers were found and installed by putting in an audio CD. It worked! Next we tried to install MythTV by adding the CD to the drive.

LUGOR.org is the web page. Meetings held on third Thursdays. Do have an installfest event once a year. They are a great source for answering your questions.

New Users Notes

by John McMillan

It was a dark and stormy night, the air crackling with intensity as eight people attending the April New Users Group fired question after question starting with one about ink cartridges. Bill Statt mentioned a web site, inkblvd that sells remanufactured ink cartridges and refill kits fairly cheap. He cited his father's purchase of two Epson 440 color cartridges at $4.00 each plus $7.00 shipping, versus $28.00 for a new cartridge at Staples. An Epson Color Stylus 600 user mentioned having purchased Staples black cartridges that required several tries before the ink began to flow and then would only print about 3 pages before apparently drying up. Bill pointed out that Epson print heads are not readily accessible should repair or replacement be necessary.

A visual scan of Bill's desktop revealed an icon for setting up JV Power Tools, a suite of programs with very extensive and easy to follow documentation including a website that contains a tutorial to teach its functions and how to use them. JV Power Tools: (a.) can find and remove unneeded files you thought were gone but are still on the hard-drive; (b.) clean your computer's registry for optimal performance and stability, often with a single mouse click; and (c.) includes automatic backup and safety features.

Bill then went on to discuss a program called Foto Angelo that is available from ACDsee for about $30 and can be used to build slide shows with sound, text and transition effects. After running a 3 minute slide show, he demonstrated Foto Angelo's simple tools like the drag-and-drop, image ordering, storyboard area that makes creating shows with this multimedia builder quick and easy. Pictures are automatically sized to the screen and there are numerous transition options such as fade out and in. Although individual timing can be established for each slide, a time line would make synchronizing sound and video easier. He compared Foto Angelo to PicturesToExe (about $24, but a free trial version can be downloaded from www .wnsoft.com). PicturesToExe also lets you package individual graphic files into a self-running slide show with background music, sound effects, and titles for each slide. The time line feature simplifies synchronizing picture duration with sound and Barry Beckham's web site offers an excellent tutorial.

A Juno user with Windows 98; Norton Anti Virus, updated weekly; and Zone Alarm fire wall reported consistently getting a message "Your current security settings prohibit running ActiveX controls on this page. As a result, the page may not display correctly." The message box, headed Internet Explorer which he did not open, appeared every time he tried to go to the web. Clicking the ok button allowed the session to proceed without obvious problems. Bill pointed out that Juno is using Internet Explorer as a web browser and felt that the security settings were on high. Some versions of Internet Explorer use a slider bar to set one level for many security settings while other versions allow independent settings for specific situations. He could not recommend a course of action without knowing which version of Internet Explorer is involved but suggested looking for Internet Options. The Control Panel; Internet Explorer tools menu; or Web Preferences in Juno's menu bar, all give access to an Internet Options button. Once there, the Security tab and the Custom Level button let you view the security settings. Bill recommended not using Internet Explorer which has had a history of security leaks and cited a personal case that required two hours of work to recover from the damage it caused. He has been using Mozilla but is considering a newer version called Firefox.

Bill also mentioned using Kartoo, a meta search engine from England with very unique visual display interfaces. Referred to as maps, they are much more graphical than the typical list response from most search engines. He finds that when investigating digital photography questions he gets a totally different set of search items. In particular it presents European information not readily found by American search engines. He also uses Dogpile, which searches as many as 13 other engines results and presents the top 5-10 finds from each of them. Tucows was also mentioned but that is a download site rather than a search engine.

The discussion turned to Adaware and Spybot, programs included in Nick Francesco's "security tango" that scan the computer for spyware programs. Adaware searches files and identifies suspicious programs while Spybot searches for spyware connections in the registry. Like anti virus programs, their definition or pattern files should be updated weekly. Since spyware may be an integral part of some desired functionality, both programs provide tools that let you control the disposition of the troublesome code. He demonstrated a Spybot search with his laptop.

A Windows 98-2nd edition user described 4 problems that were occurring randomly without any apparent reason: the system clock resets to 1990; desktop icons are rearranged; the Internet dialup connection menu opens; and the task bar disappears. Bill said these might be indicative of a virus but the user has Norton's Anti Virus which is updated weekly. Another possibility was battery failure that would cause a loss of CMOS settings when the machine was turned off..

The next question concerned running DOS programs under Windows. The shutdown menu in Windows 98 includes an option to restart in DOS. When the machine is first turned on, repeatedly tapping the F8 key will display a startup menu that includes safe mode options. Click on the one that says "Command Prompt Only". Either way, when the command prompt is on the screen, open the DOS program in the normal way. Bill pointed out that Disk Defrag and Scandisk are best run in safe mode though that may return some settings to their defaults and cause desktop icons to be rearranged.

A Juno user wondered why out going mail filled the screen from side to side but incoming mail often only used two thirds of the width. Bill said this was a function of the users E-mail processor and there was nothing the user could do to change it. It was pointed out that putting the cursor one position to the right of the last character on a line and clicking delete would likely remove the carriage return, lengthening that line. It would be time consuming to do a complete document but might let it be viewed on 1 screen.

A WordPerfect user asked why the cursor was not consistent in changing from an I Beam to an Arrow when boundaries were crossed but no one had an answer. It is interesting to note that a quick look at the Cursor file of Windows 98 showed 138 files, most less than 1 kilobyte in size but occupying 589,824 bytes of disk space. This seems like overkill since there were only 22 shapes. Some were outlines, some were solid and most came in at least 4 different sizes.

The May New Users meeting started with an extensive recital of Bill Statt's adventures in trying to get a digital camera on the Internet. After using Price Grabber, a comparison shopping site, he had more tails than Wo, the proverbial dragon. Sites advertising low prices often did not have the item in stock even though they said they did. Trying to obtain information about availability and shipping dates often led to a run around with the order taker. In one case even the presidents guarantee about shipping date was worthless. The back breaking straw was when he was told the company had a policy of charging a 15% restocking fee for a canceled order, even when they did not have the item and it had not been shipped. He had thought this group to be reputable since they displayed over 1000 reviews with only 7 negatives. Another of the lower priced sites had a large number of a specific camera on hand but they were refurbished and did not work. They shipped him one and sure enough it did not work.

A Juno user's question opened a veritable can of snakes involving the use of the terms service provider, browsers and searching. When Juno is first opened, it presents a window with three tabs: Read; Write; and Web. Read and Write deal with E-mail while clicking on Web starts to open the communication links to the Internet. If Zone Alarm is on, it questions the desire to go to the web and then asks if Juno should be the server. This gives the impression that Juno is also a Browser or Search Engine when in fact Juno invokes other software for those functions. The difference between a browser and a search engine was not clearly defined.

The user had noted that Juno had changed its search engine to Yahoo. When returning to the home page, he used to get Netscape, then more recently, MSN and wondered how to get back to that point. Bill said that Juno is now using Internet explorer as a browser and recommended changing that because of the numerous problems associated with Internet Explorer. He suggested looking for Preferences under one of the menu bar choices. The Options menu includes a Web Preferences choice that opens a segmented window that contains an Internet Options button. Clicking that button opens a tabbed Internet properties window. Under the General tab, the Home Page section lets you type in a desired home page address.

Last Month Bill had suggested downloading Mozilla's Firefox browser to avoid Internet Explorer which has had a history of security leaks. A user who did that found that some of the previous application associations had been changed without notice. Bill said that the associations could be reset by going to My Computer, > View Menu, > Folder Options and clicking the File Types tab. Scan the list for the Application to be modified and click edit, then enter the program desired and click ok. Clicking the change Icon button opens a selection of icons and when one is double clicked, it becomes the icon associated with opening the program.

Another user asked why an over exposed picture had fewer options for correction than an under exposed picture. Bill pointed out that dark (under exposed) images contain information which may not be seen because of the exposure but can be retrieved when the image is lightened. The data in over exposed pictures has been burned out and is not available to help change the image. Bill went on to say that many of today's cameras average the light from different sources thus a picture of a person at the beach or back lit by a window picks up more readings from the lighter areas which distorts the average leading to over exposure. Many of the digital cameras let you choose between averaging and spot so that when the spot is placed on the subject, that concentrates the averaging area.

As an alternative, he suggested pointing the camera at the ground at the foot of the subject, and depressing the button half way. This establishes the focus and exposure and after shifting to the desired subject, press it the rest of the way to complete the exposure.

Attention was called to the announcement of a new virus which does not involve an attachment. As such it can take effect without your opening it. It was thought that this was aimed at Window operating systems later than 98 and that active use of firewalls and antivirus programs may prevent this virus from harming your machine. Bill went on to explain that this was a problem in Windows XP and 2000, which only required an Internet connection and did not even involve E-mail. Microsoft has a patch for this on their web site. He warned against doing the critical update for XP or 2000 which will disable several features in Outlook Express.

Bill was asked to search his hard drive for On Line Services, a folder one Windows 98 user found on his machine. It contained 86 files in 8 folders with linkages to AT&T, Compuserve, Mindspring, MSN, and Prodigy, presumably inserted by the original manufacturer in hopes of selling ISP services. On Bills machine, On Line Services contained 35 files and 3 sub folders and occupied 1.54 Mb of disk space. Since the only ISP you need to get to is the one you actively use this, folder can probably be recycled for a significant space saving.

A user asked about the stability of floppy disks for archiving data. Bill compared the stability of dyes used in different styles of burnable CD's versus commercial music CD's and mentioned that professional photographers who want to archive images use gold CD's with an anticipated life of 25 years. He mentioned that since the floppy disks are an electronic medium they can degrade but suggested going to the Wilhelm Institute, a group that has done many studies on product shelf life.

A user having trouble sharing a printer between 2 machines asked how to use Network Neighborhood. The Printer was physically attached to an XP machine as it should be and a floppy disk had been made on the XP machine to install the network neighborhood on the Windows 98 computer. Both machines and the printer were turned on. Bill suggested turning off Zone Alarm to see if the firewall might be blocking the printer from working. He asked if printer folder in XP indicated sharing was on and used his laptop to go to control panel, then printers, to illustrate the question. Another possibility might be the sequence in which the computers and the printer were turned on.

Our next meeting will be June 1st at 6:30 in the Monroe Developmental Center, 620 Westfall Road.

Treasurers Report

by Steve Staub

Balance as of 4/14/2004	$837.23
Deposits	
Dues	$480.00
Donations	30.00
Picnic	20.00
Food	18.56
Raffle	17.00
Total	$565.56
Expenses	
St. Stephens	$75.00
Paper (double order)	97.30
Postmaster	100.00
Total	$272.30
Balance as of 5/18/2004	$1,130.49

The Lighter Side

Ironies

Dramatic Irony: Paul Maritz (A Microsoft VP): “We have no intention of shipping another bloated operating system and forcing that down the throats of our Windows customers”

Socratic Irony: Bill Gates: “I believe OS/2 is destined to be the most important operating system, and possibly program, of all time. As the successor to DOS, which has over 10,000,000 systems in use, it creates incredible opportunities for everyone involved with PCs.”

Just plain funny: NC World Editor-In-Chief Nicholas Petreley coined the first law of computer trade journalism: “No technology exists until Microsoft invents it.”

Open Lawsuit Foundation

In a rash of lawsuits inspired by suits by Xerox against Apple and Apple against Microsoft/HP, the whole computer industry was thrown into a tizzy when Digital Equipment, IBM, Unisys, and AT&T agreed to form the Open Lawsuit Foundation (OLF). “We are totally against proprietary lawsuits,” said a DEC spokesman. “We want standards in lawsuits.”

An IBM spokesman concurred. “We have sued everyone from little companies like Big Blue Inc. to Hitachi but we have always had proprietary suits. Now to show our leadership in the standards industry, we intend to standardize on our suits.”

When asked to comment, a Sun Microsystems representative stated, “We don’t wear suits at Sun.”

http://www.ibiblio.org/blah.html