The Cursor

Monthly Newsletter of the
Washington Area Computer User Group

Meeting Location
Fairfax County
Government Center

Member of apcug

Next Meeting:
February 23, 2008

Presidential Bits

February 2008 Meeting

By Paul Howard

January's meeting included WACUG's annual meeting and election process. Not surprisingly, the slate of candidates was elected by acclamation. My thanks to Jim Brueggeman, who served as Vice President during my terms as President, and in many other roles in WAC over the years, stepped down to a Director's slot. Jim has been invaluable to me in navigating the nuances of WAC's procedures, and helping support my hand on the tiller. Geof Goodrum now serves as VP, with Bob Rott as Treasurer, and Bill Walsh as Secretary. Volunteers are still sought to help serve the group in Board director slots.

Bill Walsh, who introduced us to Google Earth in January, will be following up in February with a DeLorme Street Atlas USA 2008 presentation. Bill plans to run through the best features of the software---point-to-point routing, location of points of interest, GPS realtime location and logging, voice command and response, map editing and printing, etc.

DeLorme has been doing maps since 1976 and its Street Atlas USA software has been around for about 15 years. Their current version is SA2008, and, as they make new releases an annual event, it becomes harder to make distinctive improvements that add value to any new edition of the software. Except for offering satellite imagery for sale for many states, DeLorme mainly offers updates and expansion for roads and points of interest; their suite of useful tools are not much better than their landmark SA2006 version.

Bill will show off a new acquisition, one of the newer self-contained GPS units that are starting to take over the market. These small mobile and handheld units that have been around for a few years are experiencing a convergence of capability, convenience, and affordability. Road maps are becoming more accurate, visuals and voice commands reliably guide you to your destination, and, increasingly important, searchable points of interest are included that help you find many places of commerce and convenience.

He will compare and contrast the DeLorme software and my new GPS unit; attendees should find this to be a fun and instructional demonstration of personal guidance technology.

Geof Goodrum and Bob Rott will once again regale us with a recap of their visit to the annual meeting of the Association of Personal Computer User Groups (APCUG), and the wonders of the Consumer Electronics Show, held in Las Vegas in

See *PresBits* page 2

Lloyd's Web Sites for February, 2008

by Lloyd Johnson, WACUG Member

http://www.wacug.org/ is the URL for the Washington Area Computer User Group. Visit it for past issues of Web Sites with hyperlinks

1. Roget's Thesaurus: http://thesaurus.reference.com/ – The thesaurus that appears on this site is Roget's New Millennium Thesaurus. To use the thesaurus, simply type a word in the gold search box and click the 'Search' button. A list of synonyms and antonyms will be returned. Related site: How to Use a Thesaurus

2. The Politico: http://politico.com/ – The Politico launched in January, 2007 with the mission of covering the politics of Capitol Hill and of the presidential campaign, and the business of Washington lobbying and advocacy with enterprise, style, and impact. The Politico is a publication of Capitol News Company, LLC.

3. The Apple Museum: www.theapplemuseum.com – Welcome to The Apple Museum. The Apple Museum is dedicated to the history of Apple Computer, Inc. and with more than 350 Apple products listed, the most comprehensive Apple history source on the internet.

4. AIRNow: www.airnow.gov – The U.S. EPA, NOAA, NPS, tribal, state, andlocal agencies developed the AIRNow Web site to provide the public with easy access to national air quality information. The Web site offers daily AQI forecasts as well as real-time AQI conditions for over 300 cities across the US, and provides links to more detailed State and local air quality Web sites.

5. Time & Life Pictures: www.timelifepictures.com – Time & Life Pictures is an unparalleled collection of striking imagery, documenting past and present events in politics, culture, celebrities and the arts. The collection includes some of the greatest photographers of the 20th century, such as Alfred Eisenstaedt, Margaret Bourke-White, Andreas Feininger, John Dominis, Nina Leen and Gjon Mili, whose photographs have adorned the pages of Time, Life and other Time Inc. publications. The online collection

6. FlightAware: Flight Tracker: http://flightaware.com – FlightAware is a free flight tracker that will change what you think about live flight tracking and aviation information.

7. Spam is spreading to cell phones. Put your cell-phone on the national Do Not Call List. www.fcc.gov/cgb/consumerfacts/canspam.html.

8. The Mitchell Report: http://sports.espn.go.com/mlb/news/story?id=3153509 – On March 30, 2006, baseball commissioner Bud Selig asked former Sen. George Mitchell to investigate steroid use in baseball. Now, the report is out and available at this ESPN site along with other related issues and resources.

9. Popular New Year's Resolutions: www.usa.gov/Citizen/Topics/New_Years_Resolutions.shtml – Suggestions from USA.gov, the official home page for the U.S. government. Drink less alcohol, get fit, quit smoking, volunteer to help others, etc. Each suggestion has links to related government sites.

10. Worldmapper:www.sasi.group.shef.ac.uk/worldmapper/ – Worldmapper is a collection of world maps, where territories are re-sized on each map according to the subject of interest

Pres Bits from page 1

January.

Don't miss this meeting - your attendance is always important !

NCTCUG

Visit our "sister" user group. The National Capital Technology and Computer User's Group meets the first and fourth Wednesday of the month. They meet in Carlin Hall in Arlington at 5711 South 4th Street. Visit their web site for more information, a map and directions:

http://www.nctcug.org/

Meetings start at 7:00 PM

GNU/Linux SIG

By Geof Goodrum, WAC

GNU/Linux Distribution Releases

GNU/Linux distributions are complete GNU/Linux operating system and application software collections. Many are freely downloadable or can be ordered on CDs or DVD at low cost. DistroWatch.com lists the following distribution release announcements for the period November 25, 2007-February 9, 2008.

Distribution

Annvix 3.0
ASPLinux 12
Astaro Security Gateway 7.1
Berry Linux 0.87
Bluewhite64 Linux 12.0r1
CentOS 5.1
CRUX 2.4
Damn Small Linux 4.2
DARKSTAR Linux 2008.1
Debian GNU/Linux 3.1r7
Debian GNU/Linux 4.0r2
dyne:bolic 2.5.2
EnGarde Secure Linux 3.0.18
Finnix 91.0
Geubuntu 7.10
GoblinX 2.6 "Micro"
GoblinX 2.6 "Mini"
GoboLinux 014
IPCop 1.4.18
Linpus Linux 9.4 "Lite"
Litrix Linux 7.12
LliureX 7.11
MEPIS antiX 7.01
MoLinux 3.2
Nonux 4.3
Parsix GNU/Linux 1.0r0
PCLinuxOS 2008 "MiniMe"
Pioneer Linux 3.1
SchilliX 0.6
Scientific Linux 5.1
Shift Linux 0.6.2
sidux 2007-04.5
SimplyMEPIS 7.0
Skolelinux 3.0r1
SME Server 7.3
StartCom Enterprise Linux 4.0.5
SystemRescueCd 0.4.3
trixbox 2.4.0
Turbolinux 11 Server
Ubuntu 6.06.2
Ubuntu Muslim Edition 7.10
UHU-Linux 2.1
Ultima Linux 8.3
VectorLinux 5.9
Vine Linux 4.2
Voltalinux 2.0
X/OS Linux 5.1
Yellow Dog Linux 6.0
ZenEdu Live Christmas Edition
Zenwalk Linux 5.0

Linux Software of the Month

The software described below is downloadable at the links provided or may be requested on the monthly CD. In addition to the monthly CD described below, WAC can provide CD-R and DVD±R media for any downloadable GNU/Linux operating system distribution (e.g. Fedora, Mandriva, Ubuntu, Debian, Knoppix). Please note that download versions of commercial distributions do not include official technical support nor printed documentation.

Discs are available only by pre-order. Contact Geof Goodrum by e-mail g (linux@wacug.org) at least 48 hours before meeting day to order or for more information. Single CD-R discs are available with a $3 donation; GNU/Linux distributions on multiple CD-Rs or single DVD±R are available with a $6 donation.

February 2008

Micropolis – http://www.donhopkins.com/home/micropolis/. Free GNU General Public License source code and executable by Will Wright and Don Hopkins. This is a complete GPL Open Source release of the original Electronic Arts SimCity™ city simulation game, supporting the One Laptop Per Child (OLPC) project.

GPSBabel – v1.3.4. http://www.gpsbabel.org/. Free GPL General Public License source code and Fedora executable package by Robert Lipe. GPSBabel converts GPS waypoint data between about fifty file formats, including Magellan and Garmin serial, Garmin USB, Mapsource, Mapsend, Streets & Trips, Delorme, National Geographic, many PDA formats, and many others. It is endian and word-size safe, includes a GUI, and runs on a variety of operating systems. It also supports Groundspeak GPX extensions for geocaching.

jGnash – v1.11.7. http://jgnash.sourceforge.net/wiki/index.php/Main_Page. Free GNU General Public license Java executable by C. Cavanaugh. jGnash is a personal finance application written in Java. A JVM of 1.4 or greater is required. jGnash supports several account types, including investment accounts. jGnash has support for split transactions, nested accounts, scheduled transactions, commodities, and currencies. jGnash can import QIF files, excluding investment accounts and transactions. Data is stored in an XML format so it is easy to manipulate and read

See *Linux* page 4

Linux from page 3

the data external to the program. jGnash also has scripting support to add custom reports and functionality.

Open Tax Solver – v5.0.1. http://opentaxsolver.sourceforge.net/. Free GNU General Public License C source code by Aston Roberts. OpenTaxSolver (OTS) is a free program for calculating Tax Form entries and tax-owed or refund-due, such as Federal or State personal income taxes. TaxSolver has been updated for the 2007 tax-year for: US 1040 and Schedules A, B, C, & D, and State-Taxes for California, North Carolina, New Jersey, Pennsylvania, Virginia, and Ohio. Soon to be released are updates for Massachusetts and New York. This year there was a delay in getting the final AMT forms from the IRS, due to last minute changes from Congress. Although OTS data entry is through text files, two optional graphic interfaces are available. The developers verify OTS results against commercial tax preparation packages.

Kernel Source – http://www.kernel.org/. 2.6 kernel source code for all platforms (stable 2.6.24.1).

Free Online Tax Preparation and Filing

By Geof Goodrum

Were you aware that you can file your US Federal and state income tax returns online for free?

Free File is a partnership between commercial tax preparation and electronic filing (e-file) services and the US Internal Revenue Service (IRS). However, this free service is only available to those with adjusted gross income (AGI) of $54,000 or less in 2007 and must be accessed through the IRS Free File web site (http://www.irs.gov/efile/article/0,,id=118986,00.html).

Not as well known is that those with AGI over $54,000 can also prepare and file their taxes online for free. The TaxACT Online service (http://www.taxactonline.com/) allows all taxpayers to use their standard online service to prepare and e-file at no charge. However, while preparing a return, TaxACT standard encourages the filer to upgrade to the $9.95 Deluxe service or the $16.95 Ultimate service, which includes State tax preparation and e-filing. The Deluxe service features import and comparison of data from a TaxACT 2006 return (if any) and W2 information, online access to J.K. Lasser‘s Your Income Tax Guide, and phone technical support (a complete feature comparison table is at http://www.taxact.com/products/all_compare.asp?v=OL).

Although the TaxACT Online Deluxe service has advantages (particularly for those with complex tax situations), it isn‘t necessary to take advantage of free e-filing. Although the Ultimate service automates much of the State return filing, free online preparation and filing is also available through state government web sites by just cut and pasting a few fields from the TaxACT Federal form.

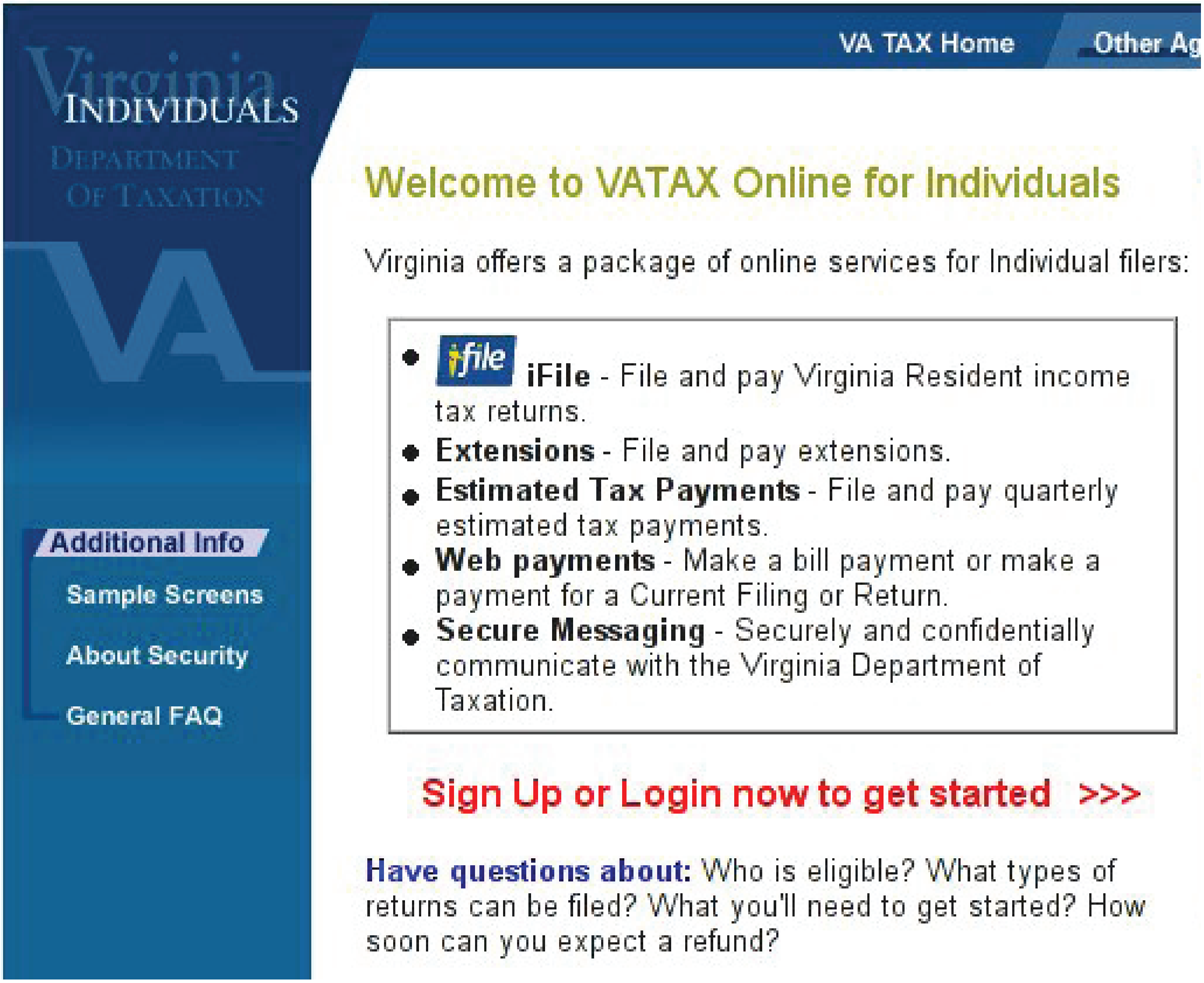
The Virginia Department of Taxation iFile service is available through the web site http://www.tax.virginia.gov/.

Maryland taxpayers have iFile service through the Comptroller of Maryland web site at https://interactive.marylandtaxes.com/Individuals/iFile_ChooseForm/default.asp.

District of Columbia taxpayers can prepare and file DC taxes through the Taxpayer Service Center web site at https://www.taxpayerservicecenter.com/individual/Ind_Logon.jsp?type=100.

I have used the TaxACT Online service with Virginia iFile for several years. Both have been secure, reliable, accurate, and easy to use with plenty of online help. Both allow the filer to stop at any time, logoff, and resume later. TaxACT Online standard identifies the appropriate supplemental documents from the IRS when I need more help. Those with dial-up Internet service may not want to tie up their phone line entering their tax information, but those with always-on service (e.g. DSL, cable) will find it very convenient. An added advantage is the online service is always up to date with any tax code changes, unlike off-the-shelf software. Just make sure that you save and print a copy of your returns, as well as any TaxACT worksheets you used that are not included in the return.

Virginia Department of Taxation iFile Service



Welcome to VATAX Online for Individuals

Virginia offers a package of online services for Individual filers:

- **iFile** - File and pay Virginia Resident income tax returns.
- **Extensions** - File and pay extensions.
- **Estimated Tax Payments** - File and pay quarterly estimated tax payments.
- **Web payments** - Make a bill payment or make a payment for a Current Filing or Return.
- **Secure Messaging** - Securely and confidentially communicate with the Virginia Department of Taxation.

Sign Up or Login now to get started >>>

Have questions about: Who is eligible? What types of returns can be filed? What you'll need to get started? How soon can you expect a refund?

Evaluating Your Anti-Spyware Program

by Vinny La Bash, Member of the Sarasota Personal Computer Users Group, Inc.
www.spcug.org
vlabash(at)comcast.net

For many years the most acute danger to your computer was some kind of destructive virus. Today the danger has shifted from software that is programmed to destroy files, corrupt programs, and disable systems to something more insidious, and perhaps even more treacherous. This threat comes in two broad categories known as Spyware and Trojan Horses.

Spyware started out as a stealth program surreptitiously installed on your system to track your web surfing habits. The developers of spyware didn't want to damage your computer. They wanted only to sell you something. That may be annoying, but there is nothing criminal about it.

A Trojan Horse is a program that pretends to be something other than what it really is. For example, a screensaver could be designed to install a program that will take over your system to forward spam to other machines. Trojan Horses have been used to initiate denial of service attacks, where the target such as a bank, credit card service or other high profile web site becomes so saturated with external requests that it cannot respond to legitimate traffic.

When selecting an anti-spyware program, start out by selecting one with a comprehensive signatures database. The best anti-spyware programs have databases that can recognize more than 750,000 dif-

See *Spyware* page 6

Spyware from page 5

ferent kinds of spyware and Trojan Horse programs. Read the documentation or call the company. This is important.

The best signatures database won't do you any good if it isn't updated frequently. The bad guys never seem to rest. They release new poison daily. Don't buy any solutions that require manual updates. You have better things to do. Insist on automatic updates.

Another important capability is active monitoring of your system. Wouldn't you rather prevent a malicious program from installing rather than removing it after the damage has been done? Avoid any program that removes infections found only after conducting a manual scan. This probably means avoiding some otherwise adequate free programs. There's an old saying about getting what you pay for. The best anti-spyware programs prevent spyware and Trojan Horses from ever being installed on your system.

Go for a program that allows you to customize your scans. We don't all use our computers in the same way. Some people require more comprehensive scans than others. If you are constantly browsing the internet, you are likely to benefit from a daily scan that checks active memory, system folders, the registry, and all hard drives. If you rarely use the internet or find yourself visiting the same six sites over and over, a weekly scan may be all you need.

You should be able to schedule unattended updates and scans. Your machine should be yours to use as you wish. Any decent anti-spyware program should be able to run in the background unattended, and not require interrupting your activities. The program should work according to your preferences, not the other way around. Choose a program that permits unattended maintenance and administration.

It's also important that an unattended scan can quarantine infections without requiring intervention from you. Why do some anti-spyware programs ask if you want to remove infections? Of course you do! Of all the features in anti-spyware programs, that is the dumbest.

There are innumerable derivations and iterations of spyware being created. This makes it difficult for even the best anti-spyware programs to catch and destroy them. If you open the Processes tab in Windows Task Manager, you will observe the Process Manager in action. You will see a list of objects running on your system. Some of them are applications like word processors. Others are mysterious entities that don't provide a clue as so what they do, but you can't run Windows effectively without them. Among them would be Windows Explorer, Internet Explorer, Media Center, Windows Mobile Control Center, and many others.

Beyond shutting down a process or resetting its priority, there isn't much a non-specialist can do with this feature. Clever programmers can create spyware that won't show up in the Process Manager. Any decent anti-spyware program has to have its own built-in process manager that will recognize, track down, and eliminate malevolent software that may not even be in the signatures database.

Anti-spyware programs should be able to monitor programs that load when Windows starts up. There are many very sophisticated spyware programs that to not show up in the Process Monitor or in Control Panel's Add/Remove section. If your anti-spyware program lacks this capability, find another one.

Assuming your anti-spyware program has the capabilities mentioned above, it is an excellent choice for individuals. However, businesses or organizations with multiple computers will require even more. Whoever is in charge of PCs will not have time to manually monitor or administrate individual machines. It is simply impractical in a large organization for support staff to visit every workstation, apply updates, schedule scans, and ensure that infestations are removed. If this applies to you, look for a program with a centralized administration console. This capability has the unfortunate drawback of being quite expensive, but the time saved generally justifies the cost.

Obtained from APCUG with the author's permission for publication by APCUG member groups

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

Look Ma No Hands

By Bruce Jacobs, Phoenix PCUG
newsletter editor
www.phoenixpcug.org
editor(at)pcug.org

This article was not typed. I dictated it using the speech recognition feature in Windows Vista Ultimate.

I have been using this feature on and off for certain applications for a while and it has its good points and its bad points.

The intent of the software is to allow the user to speak words into the computer and for the computer to recognize those words, understand that some of them are commands, and also understand that some of them are input to programs. In

See *Look Ma No Hands* page 7

Look Ma No Hands from page 6

other words, when I say the words “please save me”, the computer must decide whether to add the words to the document I am editing as if I had typed them, or add the word “please” to the document, and then bring up the save dialog box to save the document with the name “me”.

The program that is attempting to do this has two major hurdles to conquer. It has to recognize the spoken words correctly. This is helped by the training exercises. But it has its limitations.

It must also understand “in context” which of those words are commands and which of those words are to be part of my document. As time goes on, you learn to pause before speaking a command. So in the above example of “please save me”, I would say the words altogether relatively quickly in order to enter them in my document. If I wanted to add the word “please” to my document then save the document, I would speak the word “please”, then pause for a few seconds, then say the word “ save.” This would bring up the save dialog box and I could continue as if it was a command.

As far as the good points are concerned: If I’m working off printed list or when I know for sure what I want to say clearly, it can be a much faster way of inputting text than for me to type it. Some of that is due to my typing speed being somwhat slow. I am a faster typist then most hunt and peck folks, but I would never be able to keep a job as a secretary. It is also much better at spelling than I am.

If I don’t know what I’m going to say in advance the program does not facilitate me speaking what I want to say and then recomposing it later. Some of this may be my fault. I find that I can type up an article by hand and maintain enough control so that in the end I have something coherent. When I just speak out what I want it does not always make sense. I spend way too much time revising it.

One of the disadvantages is that you need to spend a little bit of time training the voice recognition system. The system works best when you are running a very simple application such as WordPad or Notepad. It can even be used to some extent in Microsoft Word. However when using an application such as PowerPoint, the program spends so much time trying to figure out what possible commands you might be wanting to perform and not enough time actually realizing that you are trying to enter words.

Another problem is homonyms. These are words that sound the same but they have different meanings in English except for the possibility of some contextual clues. There is no way for the speech recognition software to know whether I want “2”, “two”, “to”, or “too.” During setup the program asks you if they can look at the contents of documents on your hard drive to help you determine what word you used most often and in what context. This does help it guess which homonym you want.

The final problem I wish to discuss is the editing features. Whenever I create a text document I will want to fix mistakes. There are some commands in the software that will help fix mistakes, but they are limited and clumsy. Some of them will even (in theory) help prevent mistakes by the voice recognition software in future. All that being said, I find that editing documents using the voice recognition software is very frustrating. I always resort to using the arrow keys and the mouse to navigate through the document.

Vista speech recognition is a helpful tool when transcribing printed text or when words have been spoken into a tape recorder. However for initial composition of documents or editing I do not find it useful. I do not believe that I could ever learn to use it as a complete 100% substitute for the keyboard and mouse. I would not consider it a replacement if I was disabled.

Microsoft patches still another patch

By Bob de Violini, a member of the Channel Islands PCUG, CA
www.cipcug.org
rjddev(at)gmail.com

From the once is not enough department, Microsoft has, again, patched a patch. This time, it involves patch number MS07-069, which is a cumulative security update for Internet Explorer 6 installed on Windows XP Service Pack 2 only. Apparently the initial patch released on December’s patch Tuesday caused computers to experience an unexpected crash or hang upon launching Internet Explorer. If you, like I, have updating set to notify but not download and install, or if you visit the Windows Upda-

See *Microsoft Patches* on page 8

Microsoft Patches from page 7

tesite on your own once a month instead of using Auto Update, then by all means please go to the Windows Update site and grab the fix as soon as you can. The fix doesn't require a reboot; it just makes a minor registry entry to prevent IE6 from crashing again.

Internet Explorer and G-mail

Rolling right along, there was some debate during December with regards to a "vulnerability" that exists when visiting Google's web-based e-mail site, Gmail, with Internet Explorer. When the "bug" was pointed out to the computer industry media, both Microsoft and Google denied the root of the problem was with theirs. Apparently, an investigator has claimed that IE improperly stores files in its cache and that the scripting of Gmail allows this to be exploited, which would allow someone to steal any user names and passwords for Gmail that have been entered since the last time the IE cache was purged. The simple way around this is to use a browser besides IE when you visit Gmail or, if you must use IE for checking your mail with Gmail, first purge the cache and all cookies and then log in to the site. To purge IE's cache, inside IE go to the Tools drop down menu and select Internet Options. Now, in the middle of the Internet Options box, click the Delete Cookies button and click OK in the box that pops up. Next, click the Delete Files button and click OK in the box that pops up. Now click the OK button at the bottom of the Internet Options box, and you're all set. There has been no other news about this issue, so using another browser or purging IE's cache is the only solution for now. By the way, the biggest risk for this behavior appears to be if you're sharing computer access such as that which is available at a public library or a shopping mall where you pay for a few minutes of high-speed Internet access.

Critical Updates for QuickTime

For those of you who are fond of using Apple's QuickTime media player, there have been a couple of updates released in December to fix a few critical security vulnerabilities. If you only updated QuickTime once during that timeframe, you might want to visit Apple's site to get the latest update. The most recent version of the player (without the I Tunes add-on) is 7.3.1.70. While you're at the Apple site, you might want to download and install the Apple Software updater, which makes it very easy to keep QuickTime updated. Just click on it and watch it do its thing.

HP computer vulnerabilities

For those of you who have Hewlett Packard laptops and desktops, there is a vulnerability in HP's Software Update software. This vulnerability can allow an attacker to turn your computer into a useless collection of metal and plastic that's completely unbootable. HP rushed out a fix in around four days, and it's now available for your download. Computer security experts suggest installing it even if you don't use the HP Software Update function at all, as just having the software on your computer makes it vulnerable. One catch — you have to run the vulnerable software to get the update to fix it. HP has had no comment about it at all, and there's no mention of it on its Web site. Please keep in mind that the HP Software Update software is completely separate from, and unrelated to, any other updating software that is installed on the computer like Windows Update or Microsoft Update.

Windows Vista change

Shifting gears toward Vista, Microsoft has announced that, effective with Service Pack 1 for Vista due out in the first quarter of this year, those with cracked or counterfeit copies of Vista will no longer have their machines made to run in reduced functionality mode by the Windows Genuine Advantage validation tool. Instead, they'll just get nagged about once an hour to get a legal copy of Vista on their machines. Microsoft has said that this new stance is in response to customer and partner requests. Time will tell just how well this new policy goes over.

Adobe Flash patch coming

This next item pertains to a good number of folks reading this and deals with an application that runs within the vast majority of the Internet browsers in use that's called Flash. This application enables you to see animated ads and other "mini movies" within your browser. There have been a couple of very widely publicized bugs in it, one of which has been patched. The other one is under investigation by Adobe, which has pledged a fix early this year. The way I read the security bulletin, it will probably be out by the end of January, and may already be out by the time you're reading this at home.

As of this writing, the latest version of the Adobe Flash player is 9.0.115.0. This version number will, no doubt, change as soon as the second bug is patched. The Adobe security bulletin about the second patch can be found at http://tinyurl.com/2kktqs. When you get there, you'll find it on the technical side of things, but there's a section titled

"Preventative Measures for End-Users" which spells things out in plain English for the rest of us.

Obtained from APCUG with the author's permission for publication by APCUG member groups.

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

Bot-Nets

by Brian K. Lewis, Ph.D.
bwsail at yahoo.com
www.spcug.org

Keeping your computer safe while connected to the Internet is becoming more and more difficult. The "attackers" are becoming more sophisticated and are sharing more ways to get their software into your computer. Business Week recently ran an article on the major security problems expected in 2008. Unfortunately, most of them arrived long before the new year started. We have been warned for years that it was possible to recruit unprotected computers into networks that could be controlled by an external source. This recruitment network problem has gotten much worse over the past few years. It is estimated that 7% of the computers connected to the Internet have been infected with a Botnet program. So what is a "Botnet"?

A robot or "bot" software program allows a computer to be remotely controlled without the knowledge of the computer's owner. When you have a number of "bot" controlled computers it is referred to as a "bot-net". All of the computers in the botnet carry out commands issued by the network controller. Just one example of what can be done with a botnet is the sending of spam. The controller can easily have 100,000 computers in its network. So the botmaster will contract to send out one million e-mail messages. The network can then send ten messages from each of the compromised computers. With the constant connection to the Internet using cable or DSL the computer owner will have no idea that his/her computer has been the source for ten spam messages.

Now you might say that the idea that someone can control 100,000 computers in a botnet is ridiculous. However, as of October 2007 a major Internet security service had the IP addresses of over 12 million computers that were infected with bot software. There is also a newer threat called the Storm Worm bot-net that has infected millions of computers just this year. In addition to its computer recruiting ability, it has built-in defenses that are preventing security services from analyzing it. In an E-Week article it was noted that ".. Storm worm is sending DDoS attacks to not only the researchers looking into it but to anybody on their subnet, within 5 seconds of (their) initiating efforts to fight it or examine it". A DDoS attack is a "distributed denial of service" which can bring down a computer system or network by overwhelming it with messages. A very large volume of messages are sent by the botnet in a very short period of time. It is estimated that the Storm net controls over one million computers. This would make it the most powerful supercomputer in the world, exceeding the computing power of all previous computers.

People frequently wonder why anyone would want to produce viruses, worms and other kinds of Internet attacks. Years ago it was primarily because "they could do it". Today, it has become a real source of financial gain. Let's take a look at one financial resource created by controllers of botnets. On many web pages you find ads of various types that are sponsored by Google. When these ads are clicked, the advertiser pays Google who, in turn, pays the owner of a web page, usually 80% of the fee. So the botmaster sets up a web page and contracts with Google to display ads. Then, using the botnet, sends commands to the computers in its net to click on the ads. This results in payments to the botmaster. So even with a small botnet of say 5-10,000 computers, the botmaster can easily obtain $15,000-$20,000 per month in fraudulent payments. When you consider that the known botnets all have more than 100,000 compromised systems, you get a better idea of the scale of the fraud involved. This type of click fraud has been estimated to make up 5-20% of the payments made by search companies.

Another use of large botnets is extortion. The botmaster can send an e-mail to a corporation warning that a DDoS will take place at a specific time unless a payment is made. As I mentioned earlier, spam e-mail contracts are also a source of revenue for botmasters. As these networks proliferate, the sale of the IP addresses of robotically controlled computers is also favored as an income source.

So far it would appear that the only persons affected by botnets would be corporations. However, if your computer is infected, everything you do can be reported to the botmaster. Bots can incorporate "key-logger" software. That will record keystrokes, especially any related to passwords, user names or other desirable information. Another function of bot software is screen capture. It can record an entire screen and transmit the data to the botmaster. A compromised computer can also be used as a base for finding other unprotected computers to be recruited into the net. Another consider-ation is that the largest number of computers are those in the hands of private individuals. So you may be a major part of the problem if your computer is infected by a bot.

Once a computer has been compromised, the bot software is usually designed to hide and protect itself. For example it will search for and disable any other malware located on the computer or its associated network. It may also hide itself by means of a rootkit. It may also block

See *Bot-Nets* page 10

Bot-Nets from page 9

updates of any anti-virus or anti-spyware software. It may even fake the process so the user believes that an update has taken place. One of the most common modifications involves changes to the Windows host file or by changing the location of the host file and altering the registry.

There are also some traps on the Internet that can lead a user to download bot (Trojan) software without realizing it. Phishing e-mail can lead to web pages that have automatic download links for bot software. Web pages can be hijacked and links added to lead the viewer to web sites that contain "free" software links that are actually hidden bot programs. Bot programs are incorporating "social engineering" functions which serve to entice users to unknowingly download malware. People are the weakest link in the security chain. E-mail, web pages, instant messaging, social contact web sites are all used by bot malware as a means of collecting information and linking to compromised computers.

Many times the actions of a computer user are governed by visual clues. An attacker may take advantage of this by providing false visual clues on a web page or a pop-up. If the dialog box or pop-up is intrusive the user may click inappropriately just to get rid of the intruder. This can lead to the download of a bot.

So how do you know if you've been infected? The easiest way to tell is related to how you have been protecting your computer from infection. Do you have all of the following?

a. hardware firewall.

b. software firewall that checks both incoming and outgoing messages.

c. anti-virus software that is updated at least daily.

d. anti-spyware software that you either run weekly or that runs in RAM constantly.

e. keep your Windows software patches up to date.

If you don't use any of these safety mechanisms, then your machine is almost 100% guaranteed to be compromised. Even if you have taken all of these precautions, you can still be infected. However, the most effective mechanism for dealing with bots is to prevent their getting into your computer. So you have to keep the software up to date and you have to use it.

Ideally, your firewall hardware/software combination should keep you invisible on the Internet. Bot programs are constantly searching for unprotected computers with open ports. You may not be aware that your computer has over 64,000 port that can be used for communication. The most common usage are the ports in the lower range, under 1,024. However, some bots use high end ports (>60,000) for transmission of commands. One place you can check your computers port and its invisibility on the Internet is www.GRC.com. The Gibson Research site provides a free port scan and much good information on interpreting the findings as well as how to protect your system.

Ideally the anti-virus and anti-spyware software would be able to find and remove any bot software that made its way onto your computer. However, this software needs to know the "signature" of the malware in order to identify it. So the producers of the malware are always a step ahead of the good guys. The security services have to find and disassemble the new malware before they can devise the protection against it. So it is up to the user to keep the security software as current as possible to reduce the chances of infection. Like it or not, security on the Internet is a never ending battle.

Dr. Lewis is a former university and medical school professor of physiology. He has been working with personal computers for over thirty years, developing software and assembling systems.

Obtained from APCUG with the author's permission for publication by APCUG member groups.

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

Washington Area User Group Partners
Working Together For Our Members

CPCUG NCTCUG WACUG

The Cursor

Copyright ©2008 WACUG Monthly Circulation: 100

The 2007 WAC Board of Directors, SIG Leaders and other Volunteers

President:	Paul Howard, 703-860-9246, plhoward@verizon.net
Vice-President:	Geof Goodrum, 703-370-7649, ggoodrum@bigfoot.com
Secretary:	Bill Walsh, 703-241-8141, bill.walsh@cox.net
Treasurer:	Bob Rott, blbob1b@verizon.net
Director Emeritus:	Lu Spriggs, 843-467-9022, luspriggs@aol.com
Internet Support:	Lloyd Johnson, lloydhj@aol.com
Vendor Contact:	Chuck Roberts, 703-876-9787, chrobe@cox.net
PC SIG Leader/Disk Librarian:	Bob Mason, 703-503-9324, Bob.Mason@remjem.com
Linux SIG Leader, Membership Chair:	Geof Goodrum, 703-370-7649, ggoodrum@bigfoot.com
Meeting Setup/APCUG Liaison:	Bill Walsh, 703-241-8141, bill.walsh@cox.net
Web Site Team:	Paul Howard and Chuck Roberts
Newsletter Editor:	Chuck Roberts, 703-876-9787, cursor@wacug.org
Member at Large:	Mel Mikosinski, 709-978-9158, melvin22003@aol.com
Member at Large:	Jim Brueggeman, 703-450-1384, bigjimo1@aol.com

The Cursor is the official publication of the Washington Area Computer User Group (WACUG), a Virginia membership corporation. WACUG is a tax exempt organization under section 501(c) (3) of the Internal Revenue Code. Contributions are encouraged and are tax deductible. All material is Copyright © 2008 by the Washington Area Computer User Group unless otherwise specified. Products or brand names mentioned may be trademarks or registered trademarks of their respective owners. The contents of articles herein are the responsibility of the authors and do not necessarily represent the Washington Area Computer User Group, the Board of Directors, or its members.

The Cursor provides news, commentary and product information to members of the Washington Area Computer User Group.

Send membership inquiries and address changes to: membership@wacug.org
Send article submission and reprint requests to the Editor: cursor@wacug.org

WAC Membership/Renewal Application

Dues are collected on an Annual basis and includes: downloadable links for WACUG Selected Software (formeraly DOM), and WAC's monthly newsletter, ***The Cursor***, in PDF format

Individual/Corporate/Family Dues: $25.00
$12 annual surcharge for delivery of the Cursor by 1st Class mail

Remit payment in person at the WAC Membership table on meeting day, or by mail to:

Washington Area Computer User Group
30 Fendall Ave.
Alexandria, VA 22304-6300

Make checks payable to WAC. Please do not send cash by mail. ***Thank you for joining WAC!***

Complete if you name and address do not appear on the reverse side. Include E-mail Address

Name:
Street:
City:
State: Zip:
Phone: ( ) –

E-mail:

Membership Survey: Help us to help you by completing this survey. List the computer systems you own / use (in order of preference)

Operating System(s):

Modem(s):

Printer(s):

Other Hardware:

Favorite Software:

Connection: (circle one) Dial-up or Broadband

Circle Your Interests: Photo Printing Investing Games
Digital Photography Internet Access Education Music
Graphics/Animation Genealogy Video Finance
Programming Language(s)
Hardware Upgrades/Repair List others below

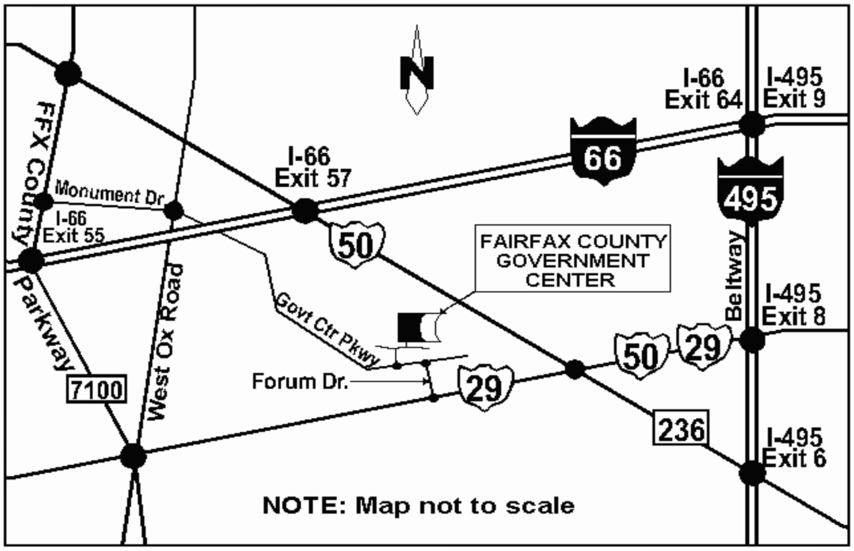
Next WAC Meetings: • Feb 23 • Mar 15 • April 19 • May 10 • June 21

Call (703) 370-7649 for the latest meeting information or Visit our Web Site at: http://www.wacug.org

February Meeting will be held at the Fairfax County Government Center Fairfax, VA

Go through front door about 25 feet then follow sign to the Meeting Room on the right

Service Desks Open at 12:30 Meeting Starts at 1:00 PM
FREE ADMISSION
BRING A FRIEND!



Washington Area Computer User Group
30 Fendall Avenue
Alexandria, VA 22304-6300
ADDRESS CORRECTION REQUESTED

FIRST-CLASS MAIL

Stamp

TIME-SENSITIVE MATERIAL
Please Deliver By
Feb 14, 2008

Label

2007 Chaos, What/ Who Wins in 2008?

By Andy Marken, Marken
Communicaitons
www.markencom.com
andy(at)markencom.com

The fun of analyzing the past 12 months is…it's easy!

But forecasting 2008 requires separating dreams from reality…early adopters from mass market.

For the early adopters the home entertainment network is here.

The converged mobile content/communications device is here.

Content when you want it, where you want it, how you want it is here.

For the mass market…it's an awkward transitional period.

2007's Time Magazine's Person of the year was … You.

The yous of the world are connected and have the choice of an almost limitless variety of online content – written, photo, music, video.

Personal content is gaining momentum. The long tail of entertainment is moving more rapidly than Chris Anderson envisioned when he wrote his first book.

The entertainment shift is making micromarket segmentation more important to manufacturers and suppliers.

Consumer advocacy / protection groups historically viewed Microsoft as the big evil one located in Redmond, WA but with tentacles around the globe. Ironically, we don't view the kind, fun-loving kids of Google in the same manner even though they touch almost everyone on the earth in one way or another multiple times…every day.

They've helped us get over concerns of privacy. In just a few minutes you can find out almost anything/everything you want to know about any company, any individual. Get over it !

To help even more they are going to make a move to build out the communications infrastructure and they'll begin offering location tracking "services" all just to help…you!

But how can you consider any of the Googlites activities/efforts could ever be used for evil when they have vowed they will do everything in their power to regreen the planet?

Jostling for Their Futures
While mobile device convergence got off to a rocky start this past year as bandwidth providers, content owners, portal services and manufacturers tried to determine exactly how they were going to get their unfair share of the consumer's dollar.

This could be a long, bloody battle because it will determine the shape and future for each segment well into the 22nd century.

The initial devices in an awkward manner let you use them to place/receive calls, watch TV/video, listen to music, track your location and handle your IM/email communications they moving target first generation products. We will see three to four generations of new products in 2008 as producers focus on key issues:

- Significant improvements in ease of use
- Fexibility in allowing users to customize applications to suit themselves
- Managing the bloating storage issues

With the explosion of content on the iNet we're seeing a dramatic increase in the demand for higher bandwidth.
Legacy applications like email and simple web browsing required relatively little bandwidth.

The three-minute call was easily handled by landline and thru-the-air phone services. But add the expectations of flawless HighDef and future Ultra HD content and video on demand and we will be faced with two options that only the bandwidth providers want to consider:

- Dramatic investment in bandwidth infrastructure (higher rates to pay for the expansion)
- Tiered services and payment schemes to support managed QoS service provisions
- Year of Storage

Because of the glut and demand for content, Time Magazine's person of the year for 2008 will undoubtedly

See *Chaos* Bonus Page 2

be…Storage !

Storage for the home.

Storage for the mobile device.

Storage for the personal stuff.

While everyone still has closets, drawers, storage sites stashed with dusty analog content; the cost and work of bringing it into the digital era is more than anyone wants to contemplate.

But today's stuff is a different matter!

The new product, new technology buzz of solutions for the home is just beginning this year and it will have a ways to go before it reaches mass market. A few manufacturers like HP are delivering first generation home network storage solutions that kinda work with and for the customer rather than in their own engineered manner.

True, you can:

- Network them
- Move content from one system to another
- Back up the stuff locally and remotely

But none of it is yet easy, natural which is required for mass market implementation. The industry over the next several years will be focusing on:

- Increasingly delivering on the promises of UPnP
- Providing self-diagnostic, self-healing storage devices
- Delivering more intelligence on deterring when content needs to be moved from one system to the home storage device and when the content needs to be archived/protected offsite

That's a heavy workload and will still require evolutionary consumer adoption until we reach a point where use is just too easy, too logical, too economic not to use.

In the meantime, 2008 - 2010 will be a great period for storage device, media, solution providers – hard drive, flash, optical.

People will still be comfortable in storing and sharing digital files on blank media. CD media sales have been flat to slightly down this past year. DVD media sales have probably reached their peak. Once we see more BD/HD DVD burners hit homes/offices we'll see the recordable media format sales increase because it is a logical extension, an evolutionary step in storage for consumers.

A DVD burner – which stores content on both CD and DVD – lasts five plus years before it needs to be replaced. That replacement price today is well under $50 today. The media costs virtually nothing. People "know" their content is archived.

While the save-and-sneakernet product market will remain stable, the hard drive/flash market will grow significantly this coming year.

Home Storage

By the end of 2008, 1TB/2TB home servers will become normal.

250GB storage in notebook and desktop systems will become standard.

80GB mobile devices will be "expected" as we use them to carry our music, photos, video, web shows, TV fare.

The biggest winner in this HD space will be the one who does more than just offers higher capacity, cheaper bit buckets.

The edge will go to the producer who can deliver diagnostic and health maintenance intelligence, not the one who can simply squeeze more data on a single platter.

Mobile Play

Flash technology which is working to find a home in lighter, more power efficient notebooks will be a niche solution in 2008. Advertised and wished for performance probably won't be achieved for 2-3 technology generations. Even with the early adopters SSD units in notebooks will be a "bragging rights" niche product until at least 2009.

But there is still an almost insatiable demand for flash based solutions.

In the coming year, "everyone" will have a couple of 8-12GB USB drives, 4-5 8-16 SD cards for their cameras, a couple of 16-24GB cards for their camcorder and 3-4 4-8GB cards for their cellphone.

Of all of the storage applications, we believe the mobile phone usage will be the most exciting and the most aggressive.

Now that the cellular services of Americas have come to realize they are service providers, not device sellers we should see a rapid succession of new mobile phones both here and abroad that will make life on-the-go easier and more satisfying.

It's also more logical for the phone producers.

If you scan the BOM (bill of materials) of a 4GB cellphone with 5MP camera and 2-3 in screen, one of the most expensive components has got to be …storage.

Remove storage from the equation, offering the consumer with "virtual storage" options and other software-ready features like music/video download, GPS, 3D screen and suddenly you have an economic device you can enjoy for years…yeah right!

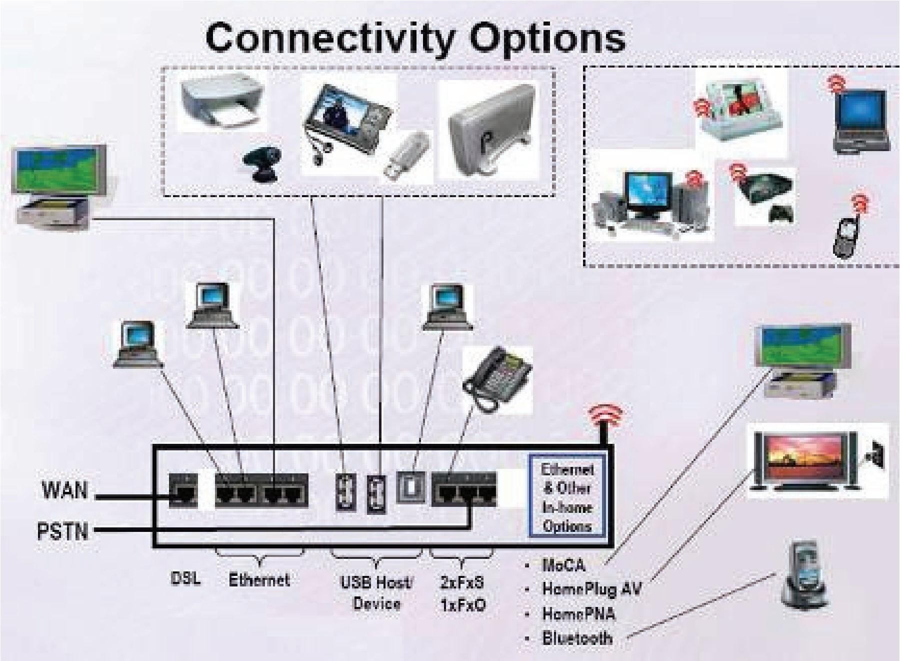
Handset manufacturers will be delivering a more feature-rich, more economic and more flexible device to the manufacturer and will place the onus to deliver low-cost, rugged capacity where it belongs…at the flash producers' front door.

At home and away the demand is

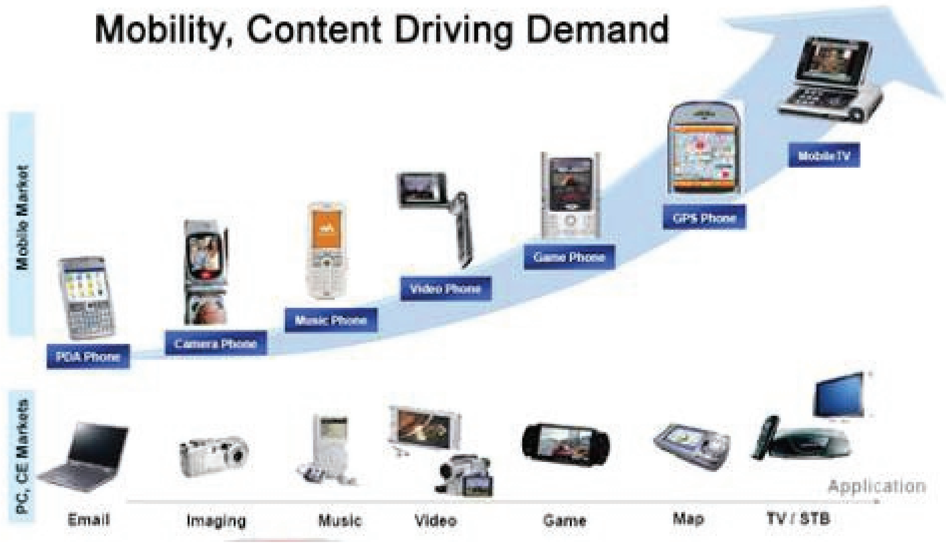
See *Chaos* Bonus Page 3

going to be connected to/using your content in new and different ways. Simplifying the process and making it cheaper, more reliable, more flexible is going to make it easier to kiss fixed providers goodbye …like the cable guy!

Obtained from APCUG with the author's permission for publication by APCUG member groups.This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).



Connectivity Options



Mobility, Content Driving Demand