OTTAWA PC NEWS

Vol. 18 number 7 The newsletter of the Ottawa PC Users' Group September 2001

PRODUCT REVIEW

PGPfire 7.1

by Chris Taylor

It is an unfortunate reality that, if you connect to the Internet and haven't done anything to protect your machine, you are a target and you will be attacked. How much damage you sustain depends on the configuration of your computer and the skill and aims of the attacker.

One way to protect your computer is to use a hardware router such as the LinkSys which I reviewed earlier this year (see opcug.ottawa.com/public/reviews/etherfast.htm). Another option is to use a personal firewall product or an intrusion detection system (IDS). I've reviewed a couple of these programs over the past few years.

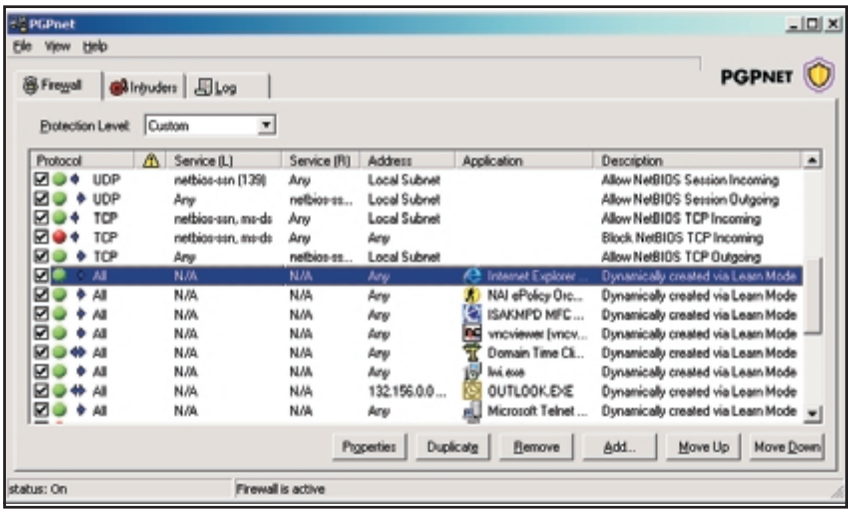
Firewalls started out at the corporate level a number of years ago. They were complex to configure and typically very expensive. Fortunately, vendors realized the need to provide a cost-effective solution for home use. Unfortunately, unless you know what you should be looking for, it can be difficult to pick out the product that protects adequately. You can get a false sense of security if you choose poorly.

An intrusion detection system (IDS), such as BlackICE Defender, looks for known attack patterns. If you want configurable protection, an IDS is generally a poor choice. It will rarely allow you to block all traffic initiated from the Internet and will almost never block outbound traffic. But it does provide protection from the specific attacks it knows about. Inadequate as your sole protection, in combination with a firewall, an IDS can be very valuable.

Most personal firewalls are packet filters. They look in the header of packets for the source and destination addresses and port numbers and protocol. Based on this information, they allow or deny traffic according to rules, either automatically configured or configured by the user.

A stateful inspection firewall goes further by also looking inside the packets to examine the packets in context. They can do things like detect HTTP (web) traffic on non-standard ports or block a particular

continued on Page 3...



INSIDE

Next meeting: **WEDNESDAY, September 12th, 2001**

COMING UP

September 12th

Office XP

presentation by Microsoft Canada

Designed for Microsoft® Windows® XP

Intel will be our guest speaker for the November OPCUG meeting.

✧✧✧

CLUB NEWS

Orphan SIG

by Henry Sims

Do you know the difference between JPEG and GIF; are you mystified by all the initials, acronyms, and buzz words computer people flash around? Can you make sense of HTML, HTTP; what do they tell you? What are PDF, MIME, XML, ADSL?

Come to the Orphans' Sig on Sept. 12, and hear Jocelyn Doire explain some of the mysteries. If there are any other expressions you need explained, let Jocelyn know beforehand at Jocelyn.Doire@opcug.ottawa.com and he will come to the meeting prepared to answer your questions.

✧✧✧

CALENDAR

Meetings	Date	Time and venue
OPCUG General Meeting	Wednesday, Sept. 12th	7:30 p.m. Auditorium of the National Museum of Science and Technology, 1867 St. Laurent Blvd.
Internet SIG (I-SIG)	Wednesday, Sept. 12th	Come and join our discussions!
Developers SIG	Wednesday, Sept. 12th	Immediately following the main OPCUG presentation, and occasionally at other locations in the region.
Delphi User Group		8:00 p.m. at Chapters Store in the Pinecrest Mall (at the Queensway)
Ottawa Paradox Users Group	3rd Thursday each month	6:00-8:00 p.m. — Corel Bldg 1600 Carling Ave
PIG SIG (i.e., Wing SIG)	Sept. 12th (after SIGs)	"Good Times" cafe at Shoppers City West, Baseline and Woodroffe

Please note that unless otherwise noted, SIGs meet at 9:00 p.m. (immediately following the OPCUG General Meeting).

PGPfire 7.1 *...continued from page 1*

combination of FTP PORT commands that you decide you don't want to allow. It is the most powerful type of firewall, as well as the most difficult to configure. I don't know of any personal firewall products that do stateful inspection.

Some personal firewalls have a learning mode that can detect inbound and outbound traffic and ask you if you want to allow the traffic. Lack of learning mode generally means that the software allows all outbound traffic. This can be dangerous. If you somehow get a trojan program installed on your machine, it can initiate a connection to an attacker's computer. The attacker can use the connection to do anything their trojan program is designed to do, such as remote control of your computer. Your firewall allows the traffic because your computer initiated the connection.

PGPfire 7.1, part of the PGP suite of security tools, seems to be a very nice balance of the various firewall options available to home users. It has an IDS and an easy-to-configure packet filter firewall. It has some base configurations with varying degrees of protection and a learning mode to handle traffic not covered by an existing rule.

When PGPfire is first installed, the firewall is disabled, which seemed a little strange to me. Once enabled, all traffic in and out of your computer is blocked unless covered by a rule.

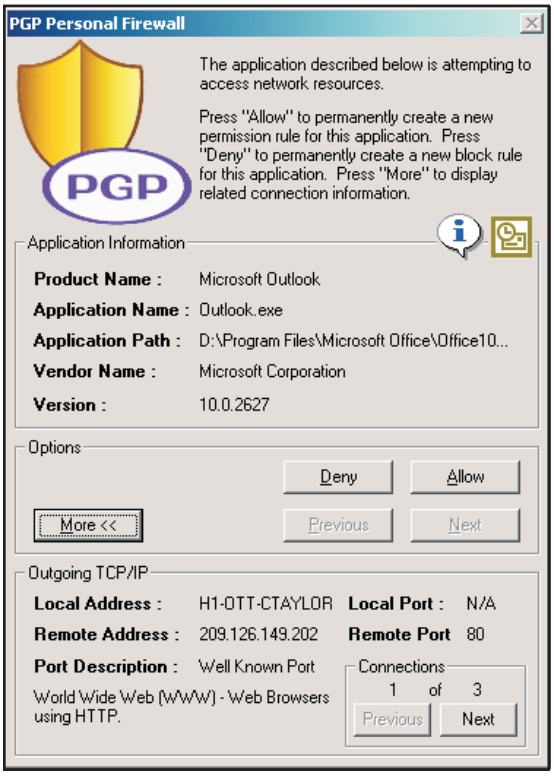
You can select from any of the predefined firewall settings or choose to create a custom configuration. The predefined levels are "minimal", two client levels, two server levels, and the default — "Learning Starter". The manual gives a good description of the levels. Any of the predefined levels may also be used as a starting point for a custom configuration, speeding overall configuration.

With learning mode turned on, when an program on your computer tries to access a remote address for the first time, PGPfire displays a dialog box with the application name and path, version number and vendor. It reports the IP address and port number the app is trying to access along with the name of the service typically used by that port, such as FTP for port 21 or World Wide Web for port 80. You choose to allow or deny the access. PGPfire then creates a rule to handle this application accordingly in the future.

If someone or something is trying to connect to your computer, the pop-up notification identifies the local program the remote process is trying to connect to along with the remote and local port numbers and the remote IP address. You can allow or deny the connection and a rule is created for the application being accessed.

PGPfire considers more than just the application name and will not automatically permit access if the program is not the same as when the

continued on Page 4...



PGPfire 7.1 *...continued from page 3*

rule was created. This is good protection against a trojan program being substituted for a trusted application.

You should review any automatically-created rule. They are typically pretty broad rules and this may not be what you really want to permit. By default, the rule will allow traffic to or from the specified local application (depending on whether the connection was initiated by the application on your local machine or from a remote address) with any external IP address using any protocol and any port. While this is usually OK, it is worth considering. Fortunately, it is quite simple to modify rules.

To edit the properties for a rule, double-click the rule in the rules list. You can specify if the rule allows or blocks traffic. You can set the protocol (ICMP, IGMP, TCP, UDP, Ipsec ESP, Ipsec AH, or All), and the direction (inbound, outbound traffic, or both). If applicable, you can specify the local application you want to allow to access remote resources or allow connections from the network. You can specify the local or remote service by service name or port. This is not a stateful inspection firewall. The list of services is there as a convenience so that you don't have to remember things like a POP3 service normally uses port 110. When you specify a service, you are really specifying the port number. You can restrict the remote IP address this rule applies to by specifying a single address, a range of addresses or a complete subnet.

One thing that PGPfire does not provide that some other personal firewall products do is to permit or deny access for a limited time or current connection only. PGPfire rules stay in effect until you manually change the rule by modifying, disabling or deleting it.

PGPfire also has an Intrusion Detection System. While nowhere near as comprehensive as a dedicated IDS such as BlackICE Defender, it is a handy addition to this package. The manual lists 17 attacks the IDS can protect you from, including Back Oriface, IP Spoofing, Ping of Death, Port Scanning, Smurf, and Winnuke. There is no indication of any way that this list can be updated to cover new attack types. If you choose, any of the filter rules on the Firewall tab can be set to be considered an intrusion.

You can configure the IDS to block the attacking source for a specified number of minutes or until you manually clear it. PGPfire can also send you an email about the attack and provide a visible or audible alarm. While I personally think it is a waste of time, you can also attempt to trace an attacker. PGPfire can attempt to find out the DNS and NetBIOS names. If the attacker is running services, PGPfire can pick up the banner from Telnet, FTP and SMTP services as well as the HTTP version. Finally, it will run a WHOIS to attempt to learn more about the attacker.

You can also manually add addresses to the Intruder list if you want to block all traffic between your computer and a particular host.

PGPfire 7.1 requires a minimum of a Pentium 166 with 32MB RAM running Win98/ME or 64MB RAM running WinNT4/2K. On my Win2K system, it generally uses about 4MB RAM and about 10MB disk space. CPU utilization is minimal. The price is CAN$105 from the PGP web site. A 30-day trial version may be downloaded from www.pgp.com.

All in all, I think PGPfire is a very nice personal firewall. Is it worth spending $105 when there are "free for personal use" firewalls available, such as Zone Alarm and Tiny Personal Firewall? Check the feature list of those other products. If they satisfy all your requirements, there is little reason to spend money on PGPfire. But don't underestimate your needs when protecting your computer.

✧✧✧

Image search engines

by Micheline Johnson

Searching for web pages based on text content is relatively easy. Searching databases or the web for images is much harder, since it is hard to define an image in a way that a search can be automated.

Indexing images manually in an hierarchical directory format, is one approach. The historical image archives at http://www.imagescanada.ca/index-e.html , and http://webgallery.nmstc.ca/ are two examples.

A more general approach uses indexing of text associated with the image, see http://images.altavista.com/ and more recently http://images.google.com/

One listing of such image search engines and directories may be found at http://websearch.about.com/internet/websearch/cs/imagesearch/

A more advanced approach involves indexing the content of the image, but here the difficulty arises not only in how to analyse and index the content, but in how to input the characteristics of the image you are searching for; i.e., how to query the search engine.

Research is being done in this field at Stanford (where I believe Google was developed) and elsewhere, see http://www-db.stanford.edu/IMAGE/

Most image content indexing seems to be based on wavelet analysis of the image. Stanford has a Wavelet Image Search Engine that is capable of searching 50,000 images per second. James Z. Wang , one of the main project group members, has an extensive list of papers on the subject at http://bergman.stanford.edu/cgi-bin/zwang/pub/show_publication.cgi?sort=3

VIPER (VIsual Property-based search Engine for image Retrieval) is a content-based image database system and WWW image search engine. The system utilizes text and visual information synthetically to support cataloging and text-, semantic- and content-based retrieval of images. In particuplar, it supports searches based on keywords, freetext, colour content, texture, and shapes. At present, the system catalogues over 12,000 images. See http://unicorn.comp.nus.edu.sg/~mmir/ . The site has demos for searching by free text, colours, wavelet transform (texture and brightness), and wavelet shape (edge detection).

Diggit! Image Search Engine, http://www.diggit.com, has 12,606,779 images indexed, which can be searched by keyword, image, URL or text. Advanced search offers a selection of image types, attributes and sizes. You can also paint queries using Active X (Diggit!FX) or Java applets (Diggit! Graffiti)

Stanford also has a paint query method of searching for other like images, see http://bergman.stanford.edu/~zwang/project/imsearch/pasearch/

Here, you draw a very simplified version of what you are looking for, and post it on your own web site, and give the search engine the URL of your sketch image. There are sample demo sketches to try, such as: Black is a don't care colour, and is not used in the search.

There is a list of Content based Image Retrieval Systems at http://www-dbv.informatik.uni-bonn.de/~gerdes/CBIR/

There is also work being done on audio and video search engines and indexing based on content.

✧✧✧

Prize winners

by Mark Cayer

From our meeting of **May 9, 2001**: Raymond Martineau received a copy of Office XP as did Keith Martinsen. The raffle prize, a copy of VMWare, was won by Allen McNamara.

From our meeting of **June 13, 2001**: Walter Josephy took home an Olympus digital voice recorder. Ted May won the raffle for a copy of VMWare and a copy of Win2000. And anyone who wanted one could take home an Olympus Pen!!

Congratulations and many thanks to all of the prize contributors.

Hexing text

by Dunc Petrie

Here's a strange one — always seems to happen when helping a friend. The job: update several files from WordPerfect 5.1 for DOS to WordPerfect 2000 format. Since WordPerfect 2000 has import filters for these files (and a smorgasbord of others) no problems were anticipated. Source media was a 5.25 inch 1.2 MB floppy; I volunteered since I had a 5.25 inch high density floppy drive. There were no read errors. For unknown reasons, these files had no extension; at least, none was visible on-screen when the directory of the floppy was displayed (but see below).

The files were copied to a subdirectory on a hard drive without problem. Curiously, when the files were viewed in Windows Explorer they were identified as Microsoft Access Table Shortcuts. Given their date of origin, Access was, at best, vapourware. No extension: no parent application. This should have opened a dialog box to ask what application should be associated with the file. Since this didn't occur, something was supplying hidden information (I have turned off the option to hide the extension of common filetypes) — but what?

Ignoring the significance of this assigned file type, I attempted to open the file in WordPerfect 2000 with mixed results. Using File Open and toggling the Preview Window 'on' I could view the entire contents of the file and scroll anywhere inside it in the Preview Window. When I clicked on the Open button, I got a dialog box: "[filename] references an item that does not exist. The item will not be returned to the application [WordPerfect]". No luck — but there is something; I can see it!

Perhaps assigning a file extension will restore order. I tried '.doc' (the WordPerfect 4.x & 5.x DOS-era default), '.wpd', '.rtf' and '.txt' but only succeeded in increasing my frustration. I removed the '.txt' extension and tried viewing the file using KeyView Pro. KeyView can view a lot of file formats but skipped this one.

Then, I replaced the '.txt' extension: still no response. NotePad tried but surrendered: "File not found. Please verify the correct name was given." Again, trying each extension in succession had no effect. MS Word 97 — the proprietary owner of the '.doc' extension — simply ignored my requests to open it: regardless of extension. MS Access 97 (supposedly the parent application) produced a blank screen. WordPad did nothing. I have run out of applications or utilities to use.

Hmmmm — would WordPerfect 5.1 for DOS run on a 32 bit FAT hard drive? Would I have to reformat a logical partition using FAT16? What about the speed of the Pentium II processor? This old WordPerfect was born in the age of *8 MHz* system buses, *huge* 30 MB hard drives and *one* MB of total system memory. Where are my DOS disks? Do I still have WordPerfect 5.1 for DOS? How do I save a file in WordPerfect 5.1 for DOS (no cheatsheet). Surely, there has to be an easier way.

Finally, a solution: why not try a hex editor? Long before C++ a lot of code was written in hex. In the days of hex, programmers counted using 16 fingers — truthfully, I am not a programmer and have no idea how they did it. One nice thing about a hex editor, it can read practically anything (Aside: have a look at a blank, formatted diskette). Peter Norton was one pioneer: Diskedit.exe survives as a command line only utility to this day. Those who used Central Point's PC Tools or Mace Utilities had similar programs and a flood of shareware offerings were also available. I needed something a bit more recent and found Ultra Edit (www.ultraedit.com), a combination text, hex and HTML editor. While the screen was full of hex this utility had three essentials: first, it was a Windows application; it could load the file without protest; and, it could 'Save As Text' although the format left something to be desired. I used Ultra Edit to read it and saved the data as a text file. I had to do some editing to remove stray characters and spaces. Strangely, all the files when viewed in the hex editor's File Open dialog box now have the extension '.MAT' (no idea of the origin of the extension).

Since '.MAT' indicates a Microsoft Access Table Shortcut (verified at http://extsearch.com) then I would have expected Access to open it or state that its file was corrupt — anything but silence. The Preview window in WordPerfect displayed text but something prevented the file opening. Also unanswered is the explanation for the hidden extension; although invisible it must have been acting behind the scenes.

My friend uses no MS Office applications (of any vintage). How did the files acquire this extension or format? It's possible that the file is an MS Access version other than 1997; file formats in the MS Office camp do change — often with each release — and the filters may be only partially successful (or not installed). Despite the unanswered questions the files were recovered. Better, I suggest that you keep Ultra Edit (or a similar program) handy for that impossible task.

✧✧✧

Four is not enough

by Dunc Petrie

Given the diversity of storage media — hard drives, optical (most commonly CD-Rom, CD-R & RW although various writable or re-writable DvD formats appear on the horizon), Jaz (and its newer variants like Orb and Peerless), Zips, LS120 and tape — it soon becomes a challenge to find adequate connectors. If your system, like most for home or SOHO, employs some flavour of EIDE then you may quickly reach the four device ceiling. In addition, only one device on an EIDE channel can be active at any instant. With multiple drives, it becomes a challenge to install the devices in a configuration that provides maximum flexibility.

Options

- Upgrade existing drives for a single, larger hard drive,
- Use a sled or tray to swap out devices (probably hard drives) on the existing controller,
- Obtain a SCSI controller card and employ SCSI drives (SCSI devices are more expensive than their comparable capacity/capability EIDE counterparts), or
- Add an expansion controller card.

Depending on your circumstances, several options, singly or combination, might prove viable.

This article will specifically address the addition of another controller card. Only a few years ago the on-board IDE controller was a single channel that accepted two devices (a master and a slave). The original specification was upgraded to include another channel — now, a primary and a secondary — with space for a master and slave on each one (total of four devices). This arrangement is commonly found on most Pentium II and Pentium III motherboards (and their AMD contemporaries). Although not contingent per se upon Ultra ATA100 some new motherboards (for example, ASUS' A7V series) have added a second on-board EIDE controller to allow you to connect up to eight devices (four channels: two primary, two secondary) on the system. Usually, one controller is Ultra ATA100 and the other Ultra ATA66.

Many computer hobbyists with Pentium II or III processors use motherboards with the Intel 'BX' chipset that implemented the Ultra ATA33 specification. While certainly capable, it has been left in the wake of both Ultra ATA66 and Ultra ATA100. Today, new Ultra ATA33 drives are impossible to obtain and even ATA66 specification drives are almost extinct. Thankfully, regardless of the 'Ultra' level all hard drives are backwards compatible; in other words, an ATA100 drive will happily run on an ATA33 controller — at the slower speed. There is an important caveat: while the connection may be compatible there are potential issues (that are not within the scope of this article) due to the new drive's large capacity and system BIOS constraints.

For those who would like to install more devices or reap the incremental performance increase of a new drive despite system constraints (including system BIOS constraints on hard drive capacity), here is an inexpensive solution (about $65 Cdn including taxes). Promise Technology's (www.promise.com) Ultra100 TX2 is a PCI slot expansion card that adds the capacity for four drives (need not be ATA Ultra100). It works with a wide range of operating systems (see features) and is easy to setup.

Requirements

- Free 66 MHz PCI slot (works with 33 MHz PCI bus but performance will suffer)
- Plug and Play BIOS
- PCI 2.1 specification (not earlier)
- bus mastering enabled

Features

- Works with many operating systems: including Windows 2000, NT4.x, Windows 9x, Windows Me, Win 3.xx, DOS (!), and Netware servers (No word about Linux or Windows XP but visit the tech support section on the website).
- Dual independent channels and timing registers prevent slower devices on the same channel degrading throughput.
- Co-exists with on-board controllers.
- Flashable BIOS supports drives up to 128 GB capacity (avoids system BIOS restrictions).

First, backup your system; in particular all the partitions on the physical drive or drives that you intend to connect to the Promise card (see 'Issues' below for the reason). Despite this precaution installation on my system (Pentium II, BX board, running Windows Me) was quick and hassle-free. I installed the card; jumpered the devices and connected them; then, powered up and installed the software driver — all done! The included driver was current; however, it never hurts to check the website for a more recent version.

OTTAWA PC NEWS

Ottawa PC News is the newsletter of the Ottawa PC Users' Group (OPCUG), and is published monthly except in July and August. The opinions expressed in this newsletter may not necessarily represent the views of the club or its members.

Member participation is encouraged! If you would like to contribute an article to *Ottawa PC News*, please submit it to the newsletter editor (contact info below). Deadline for submissions is three Saturdays before the General Meeting.

Group Meetings
OPCUG meets on the second Wednesday in the month, except July and August, at the National Museum of Science and Technology, 1867 St. Laurent Blvd, Ottawa. Meetings are 7:30–9:00 p.m. and Special Interest Groups go until 10 p.m.

Fees
OPCUG annual membership: $25 per year.

Mailing Address
3 Thatcher St., Nepean, Ontario, K2G 1S6

Web address
Http://opcug.ottawa.com/

Bulletin board—the PUB II (BBS)
Up to 33.6 kbps V.34 228-8951

Chairman and System Administrator
Chris Taylor ctaylor@nrcan.gc.ca 727-5453

Meeting Coordinator
Tim Mahoney timothyr@cyberus.ca 225-2630

Treasurer
Vince Pizzamiglio vince@monisys.ca

Webmaster
Brigitte Lord opcug@iname.com

Secretary
(Mr.) Jocelyn Doire Jocelyn.Doire@opcug.ottawa.com

Membership Chairman
Mark Cayer Mark.Cayer@StatCan.Ca 823-0354

Newsletter
Bert Schopf (editor) bert@blackbirdpcd.com 232-8427
(Mr.) Jocelyn Doire (distributor, electronic version):
Jocelyn.Doire@opcug.ottawa.com

Public Relations
Morris Turpin mturpin@igs.net 729-6955

Facilities
Bob Walker skywalk@iname.com. 489-2084

Beginners' and Windows SIG coordinator
Duncan Petrie petried@zdnetonebox.com 841-6119

Internet SIG coordinator
Bob Gowan gowanb@inac.gc.ca

Paradox SIG coordinator
John Ladds laddsj@statcan.ca 951-4581

Delphi SIG coordinator
Stan Isbrandt isbrandt@trytel.com . . . 992-8141 / 729-7793

Orphan SIG coordinator
Henry Sims ha4326@home.com

Developers' SIG
Bob Thomas BobThomas@msn.com

An 80 conductor (but 40 pin) cable — essential for ATA66 and beyond — is included along with a manual that details setup for all the operating systems.

Issues

Ultra100 (no TX2 suffix) and Ultra66 cards are also available although the latter is hard to find in retail channels. I don't know the distinctions between the 'TX2' and its earlier (non-TX2 suffix) counterpart but I advise purchasing the most recent. Shop around: I purchased the Ultra 100 TX2 for less than some outlets were offering the older Ultra66.

The website FAQ and tech support areas address some problems with Windows 95B and C, some motherboard/chipset combinations (primarily driver versions) and Windows 98 shutdown.

Finally, in some cases a boot drive that is shifted to the Promise card will not load the operating system. This is a problem with drive geometry translation (and a major hassle if it happens to you) but it does not indicate a faulty Promise controller. Although I re-routed my boot drive through the Promise card I did not encounter this problem. Remember, I did caution you to backup.

Conclusion

Promise offers an easy, inexpensive upgrade to add additional drives or to provide a modest increase in performance. While speed is always welcome — it will be less than the raw numbers suggest (An Ultra ATA100 drive will definitely not deliver sustained transfer rates that are three times those of Ultra33). Instead, I was more impressed with the greater flexibility (spreading devices across four channels) that the card delivers. During boot-up the screen displays the status of the card and enumerates the devices that are attached to it — a handy diagnostic. Everything you need is in the box; it appears well-made and offers a two year warranty.

✧✧✧

CLUB LIFE

Reduce, Reuse, Recycle

Bring your old computer books, software, hardware, and paraphenalia you want to **GIVE AWAY** to the General Meetings, and leave them at the table near the auditorium's entrance. *Please limit magazines to publication dates of less than two years old.*

You may **TAKE AWAY** any items of use to you. Stuff left over at the end of the meeting will be sent to the recycle bin.