

The Bridge

The Journal of the Memphis PC Users Group

Volume 19 Number 10

October 2003

For group information
please visit our Web site:
www.mpcug.org

The Bridge Staff:

Editor
Gil Hennon

Review Editor
Rick Fischer

Publisher Emeritus
Les Owen

In This Issue

The School Bell	Page 2
Linux in a Nutshell	Page 4
Thanks to Lynn Huggins	Page 5
Nov-Dec Meeting Preview	Page 5
eXtendia PC Firewall	Page 6
Microsoft Links 2003	Page 8
Spyware Ate My Processor	Page 10
Microsoft Optical Mouse	Page 14
Out For Review	Page 15
Linux Server Hacks	Page 16
Please Help	Page 17
MPCUG Event Calendar	Page 18

Main Meeting Wednesday, Oct. 22 Southwest Tennessee Community College

5983 Macon Cove, Memphis

MEETING LOCATION

Farris Meeting Room A

Second Floor - Farris Building

New Users & Wizards 6:30 p.m.
Main Meeting 7:30 p.m.

Trick or Treat!

The October Meeting topic
was not announced before
we went to press.

*But we always have a good
time, so come along and
bring a friend!*





The School Bell

News From MPCUG Education Services

By Gil Hennon, Education Services Coordinator

Only a month and a half ago nearly the entire Windows-Intel computing community spent about a week battling the Blaster worm and its cousin, Nachi. Both of these worms exploited an operating system vulnerability. Even though a patch to fix the vulnerability had been available for several weeks, lots of computers were infected and networks were clogged by the aggressive worms. Microsoft has been both panned and praised for its response to the threat. On the one hand, the vulnerability was Microsoft's fault. On the other hand, they provided the patch in plenty of time to kill the threat easily. In the end, because the company had no idea how many un-patched computers might participate in a denial of service attack against its Web site, Microsoft used a name server trick to shunt transactions away from its servers.

In the days that followed, incidents involving the two worms dropped to just about none. Anti-virus programs were winning the fight against Blaster and Nachi, and it looked like just about every computer had finally been patched. It looked that way, but maybe it wasn't so. Yesterday I heard about a company that was just being hit by the worms. Their network was overloaded and their email server went down. Obviously there are pockets of un-patched vulnerability still out there.

Today, Brian Livingston (www.briansbuzz.com) followed up on a previous report of another Microsoft vulnerability with more bad news. Although this vulnerability in Internet Explorer has been known for some time,

and Microsoft has a patch for it (security bulletin MS03-032, June 2003), the patch does not fix the problem. Now Brian has learned that a malicious Web page has been exploiting this security hole by downloading a program onto vulnerable computers that hijacks AOL Instant Messaging accounts. Another Web page uses the same method to secretly switch users' dial-up accounts to a \$5 per minute "pay-per-call" telephone number.

Because these new intrusions exploit Internet Explorer and are performed on Web sites, they are not associated with any worm or virus. Anti-virus tools are as unaware as the user that the computer has been compromised. Once malicious software has been installed, the machine can receive and run almost any kind of program, including hacker favorites like keystroke loggers that capture passwords and credit card account numbers.

Until Microsoft can deliver a reliable patch, Brian recommends a temporary work-around that disables Internet Explorer's "active content" functions using the following steps:

1. Start Internet Explorer. Select Tools, then select Internet options.
2. Click the "Security" tab.
3. Highlight the "Internet" icon and click the "Custom Level" button.
4. Scroll to the "ActiveX Controls and Plugins" area.
5. Under "Run ActiveX Controls and Plugins" click "Prompt."
6. Click "OK" to return to Internet Explorer.

Brian cautions that this work-around will not be convenient. Every site that attempts to use an ActiveX enhancement is going to display a dialog box asking permission to run the object, so install the patch as soon as it is available. If you find that you are clicking "Yes" often, use these steps to add a frequently visited Web site to your "Trusted Zone:"

1. Start Internet Explorer. Select Tools, then select Internet Options.
2. Click the "Security" tab.
3. Choose "Select a Web content zone to specify its current security settings."
4. Click "Trusted Sites," then click "Sites."
5. Clear the checkbox labeled "Require server verification (https:)" . . ."
6. In "Add this Web site to the zone," type the URL of the trusted site.
7. Click the "Add this site to the zone" button.
8. Click "OK" twice to return to Internet Explorer.

A site Brian definitely recommends you add to the Trusted Zone is <http://windowsupdate.microsoft.com> where you will eventually have to go to get the patch. If you do not put the Microsoft Update site in your trusted zone, or remember to enable ActiveX content before you go there, all attempts to install patches will fail.

Brian Livingston has been reporting on Windows and Microsoft issues for many years. His is one of the best sources of reliable information on the Web. I recommend him highly. To sign up for his weekly newsletter, go to <http://briansbuzz.com/w/signup/>

MPCUG Education Services has lots of useful tips for keeping your computer secure and happy. Join the Wizard session each month prior to the main meeting. For every question, there really is an answer out there somewhere!

***What we anticipate seldom occurs.
What we least expect generally happens.
- Benjamin Disraeli***

This newsletter is a monthly publication of the Memphis PC Users Group, Inc. (MPCUG) Copyright ©1998 MPCUG. Unless otherwise indicated, articles may be reprinted in other non-profit publications without express permission, subject to the following conditions. Full acknowledgement must be given to the MPCUG, The Bridge, and the author. The article must be reproduced in its entirety from magnetic media, without editorial changes, deletions or additions. Two copies of the entire publication containing the reprinted article should be sent to The Bridge within 30 days of publication. All other rights reserved. Any changes to the article require the written permission of the author. All articles are made available through the APCUG BBS and on disk to qualified non-profit organizations.

Any opinions expressed belong to the author and not the Memphis PC Users Group, Inc. Articles in this newsletter may contain trademarks of various companies. Any proprietary right those companies have in those names is hereby acknowledged.

Unless otherwise indicated, all submissions to this newsletter become the property of Memphis PC Users Group, Inc., and are subject to editing by the staff. The MPCUG reserves the right to determine the suitability for publication of all items received.

Members are encouraged to submit articles for publication. By submitting articles, the author gives permission for publication in this newsletter and for publication by other user groups. The editor cannot guarantee that all submissions will be used.

The information contained in this newsletter is believed to be correct and accurate; however, the Memphis PC Users Group, Inc., cannot and will not assume responsibility for the consequences or errors contained in articles or misapplication of any information provided. Any information used from these articles is at the user's own risk. If a review of any hardware or software contains errors or inaccuracies, upon notification of these errors or inaccuracies by the manufacturer in writing, a correction will be printed in the subsequent issue following receipt of these corrections.

The Memphis PC Users Group, Inc., makes no warranty, expressed or implied, as to the suitability of any advertised product. You must determine that yourself. The Memphis PC Users Group, Inc., also expressly declines to assume liability for any use of any published software, and your use of same constitutes your agreement to hold us blameless.

Memphis PC Users Group, Inc.
P.O. Box 241756
Memphis, TN 38124-1756
Internet: www.mpcug.org
Information Line: 901-375-4316

LINUX in a Nutshell (4th Edition)

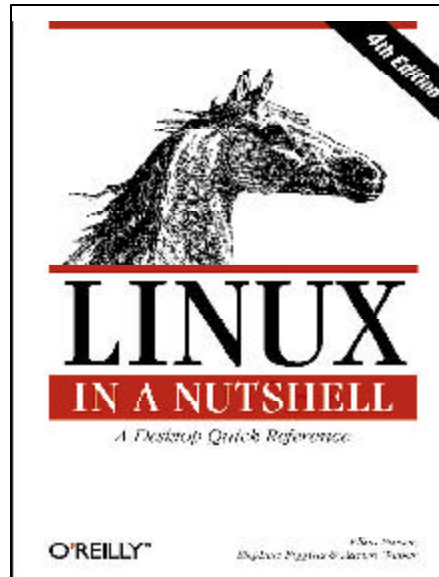
Book Review

Reviewed by Thad Craig

This is a quick-reference guide for ALL distributions of *Linux*. To my way of thinking, that in itself makes it very valuable. It was NOT written with any specific distribution (i.e., Red Hat, Mandrake, SuSE, Caldera, Debian, etc.) or any certain “version” in mind. Instead, it applies equally well to any of them and it still has the information you need 95 percent of the time. You may be familiar with other “Nutshell” books from O’Reilly publishers. Overall, I think they have an excellent reputation.

This book is extremely well organized and uses conventions common to most computer books. It offers tons of quick support to the technician who is familiar with the tasks involved. Even though it contains a very brief “beginners guide,” the book is written as a reference guide for intermediate and advanced users. You really don’t have to read it from cover to cover.

The book is amazingly complete and detailed considering it covers so many different versions and distributions! The more I looked for different areas of coverage, the more



I was pleasantly surprised. Some of the subjects included are: system and network administration, ALL Linux commands & options, boot methods, package managers, shells and scripting, text editors, and more. The only areas the book does not cover are the graphical tools such as OpenOffice, StarOffice, etc. or programming languages such as *Java*, *Perl* and *XML*. The authors explained the mere size of such coverage would have exceeded the binding limitations.

Again and again I was really blown away by all the information bound together in the book. I even looked for small areas I had seen missing in other references — and they were all there! To top

it off, the authors frequently made additional references to other books, magazines, and even Web sites to offer additional information. These authors did an awesome job putting this book together and for many, it will be a very valuable tool.

I personally consider this book to be one of the best I’ve seen and I am proud to include it as a part of my reference library. I believe it is well worth the price.

But, remember, if you do a book review for our Group, you get to keep it for yourself! If it is a good book, that is a good payment. Also remember that as Group members, we get discounts of 20% on all O’Reilly books and that can also add up to some good savings too! See below.

LINUX in a Nutshell,
4th Edition by Siever,
Figgins, and Weber.
O’Reilly 2003. 896 pages
plus index. \$40 retail.

O’Reilly User Group
Discount.

20% on all O’Reilly
books and conferences
when you order direct.
Include your User Group
code: DSUG

www.oreilly.com

A big THANK YOU to Lynn Huggins . . .

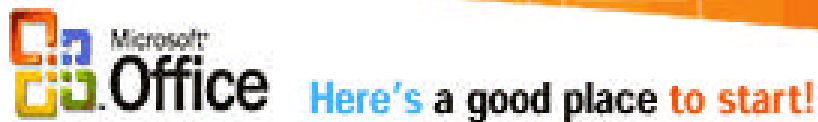
Last month when we reported that Bill Cavanaugh, Director of Career Services at Southwest Tennessee Community College, had agreed to sponsor the MPCUG for facility use, I was unaware that he had also enlisted a capable co-sponsor, Professor Lynn Huggins. Her co-sponsorship gives our group representation in STCC's Information Technology department. She was formerly a MPCUG member until her Wednesday evening classroom duties precluded her attendance at meetings, but Lynn is still very familiar with our organization and activities.

She has already jumped right into action and reserved our meeting space through 2004! So let's give a great big MPCUG round of applause to Lynn for graciously volunteering to co-sponsor and help the Group. Also, if you find you need to update up your computer skills to qualify for a promotion, or want to spiff up your resume with some additional credits, talk to Professor Lynn about the great IT classes STCC offers!

Again, many thanks and a salute from The Bridge to Professor Lynn!



November-December Meeting Preview!



At the combined November-December meeting on December 3 we will participate in Microsoft's "Sneak Preview" of Office System. Mike Davidson will demonstrate features of Office System that maximize home and office productivity. Don't miss this opportunity to see the latest and greatest in office software technology—Microsoft Office System!



By John Schuster

In this day of Internet connectivity, there are many great conveniences at our disposal. We can access information (accurate or otherwise) on almost any subject, see images of things far away (even cosmically speaking, if you look at the Hubble Space Telescope images) and read things that would not have been available, to the average person, ten years ago.

BUT, with all this comes some danger. We are inundated by SPAM, and viruses attempt to violate the privacy and security of our personal computers. This is especially true for those who are connected to the Internet at all times – either through a network (such as the one I use, here at Ole Miss), a cable modem (such as Roadrunner in Memphis) or DSL service (from your local phone system). These people's computers are a handy target!

Enter the personal firewall. First, let's define a computer firewall. It is a method or device that regulates the level of trust between two or more

networks. A firewall can consist of software, hardware or a combination of both. In this category, there are various levels of protection. They vary all the way from simply determining what applications are permitted to access the Internet (and I'm not at all sure that this would really fit the description of a firewall that I found on the Internet), to full control over what ports may be used and even what specific other computers may have access.

PC Firewall by eXtendia falls into the first category. This means that it, primarily, controls what applications are permitted to access the Internet. Can this program protect you from hackers? Not that I've been able to determine! The reporting facilities only tell you what applications have had activity on the Internet. They do not report what ports have been used or if any attempts at intrusion have been made.

By contrast, I have tried the free version of *Zone Alarm* (another personal firewall product) and it DID report intru-

sion attempts and port activity.

Shortcomings abound in this program:

1. As mentioned, above, there is no protection from outside intruders.

2. On startup, the program's control panel opens and, with this version, there is no way to prevent this (their support states that this is being remedied in the next release).

3. The reality is that this may not really be a firewall program. It is simply an application access control program.

Just for information, I looked for other information about this program and found only an advertisement, claiming:

"Your Complete Defense Against Hackers When connecting to the Internet, maintaining security is vital. Users need a powerful, yet easy to use solution that provides protection from Internet vandals and hackers. eXtendia *PC Firewall* protects your system from outside intruders or hackers attempting to access your system and it's easy to install and use. Don't take

any chances. This program is everything you need for complete PC security. Intermediary Firewall controls inbound and outbound traffic Intrusion detection system stops hackers from accessing files Security Monitor displays Internet activity Parental Control blocks unauthorized Web sites Automatic warning notification when programs attempt unauthorized Internet connections Creates evidence logs of your Internet activity by program.”

When compared with the information, on the box, I'm led to believe that this is NOT direct ad copy from eXtendia. Of these claims, I could only determine that it does control application access and warn when an unauthorized program attempts to access the Internet. The claim of blocking unauthorized hackers could not be verified. “Parental Control” of web-sites is not included in this product but is included in their companion product, *PC Ad-Blocker*. However, the back of the box does make the following claims:

1. Complete protection from the Internet through an intermediary firewall that stops intruders or hackers attempting to access your system. (There seems to be no way to



verify this short of a real lab with other computers set up to attempt hacking.)

2. The ability to select which programs are allowed to connect to the Internet – no port configurations required. (True.)

3. A continuous and invisible Intrusion Detection system that STOPS hackers from accessing your files. (Again, could not be verified – it's so invisible that they don't even log intrusion attempts.)

4. Collection and display of Internet traffic information as it happens. (This consists of a list of the applications which accessed the Internet, with sent and received byte counts; there were no log entries related to access attempts from outside, even when, as I mention later, I had an intentional

vulnerability probe of my system done.)

5. An easy to use interface that lets you authorize Internet transmission and issues a warning for unauthorized transmissions. (This one is true and accurate.)

6. A Complete Traffic Manager to graphically display your Internet traffic. (Pretty much useless as it just shows the activity level, no detail.)

7. A powerful new technology that simplifies your privacy concerns. (I cannot prove or disprove any of these statements.)

8. A multi-layered defense against unwanted attacks. (Again, cannot be verified with my level of testing. I don't have any local hackers to try to violate my system.)

9. Expandable security! Lets you add-on filtering and system cleaning capabilities. (In other words, their other applications will integrate into the same control panel.)

I did have one of our network group specialists run a probe of my system, from his Linux computer. He stated that this computer is pretty well locked down and that it would take someone with a great deal more skill than he has to break into it. I had him repeat the process after un-checking the “Enable Firewall” box, in

the control panel. There was no change in the security of my system, from outside. Thus, I still cannot attest to the claims of protection from outside intrusion.

Note that I do keep this computer fully up to date with Microsoft security patches. These, I believe, have a strong bearing on low vulnerability of my system. I will continue to use *PC Firewall* until something else comes along for me to look at.

The bottom line is that I would not assume this program to offer FULL protection to your system without the additional steps of keeping your security patches and anti-virus definitions up to date. If you need good logging of attempted break ins and probes, this is not the program for you. The people, who want to hurt you, are not holding back on using everything they can. Neither should you!

PC Firewall is a product of:
Boomerang Software, Inc.
90 Concord Ave.
Belmont, MA 02478
(617) 489-3000 x 118
www.eXtendia.com

Suggested Retail Price:
\$29.95

Microsoft Links 2003

Software Review

Reviewed by Mike Dudas

Links by Access software and *Golf* by Microsoft have been through several editions with the Access product using a game platform and the Microsoft product using the *Windows* platform as far back as *Windows* 3.0 and the 386 processor. One interesting feature is that the "add on" courses have been compatible with both products.

Over the years, the updated programs have provided patches so that most of the courses would be available if you had purchased them for earlier editions. Newer courses generally have more advanced graphics and are more realistic.

Installation

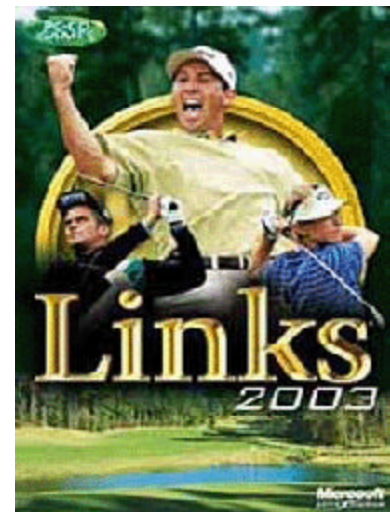
Installing *Links 2003* involved the usual: insert the CD and allow AutoRun to operate. When it came time to run it, I was told that direct 3D acceleration was not properly installed. I determined that this was because my video card (NVIDIA RIVA TNT2) did not have the latest drivers. With the help of Google I found what I needed. The readme file mentions there are some DirectX

issues with some video cards including NVIDIA cards. Fortunately it didn't affect my card. Now, I was able to load courses and play.

The Courses

Links 2003 has six courses. Two additional courses are available as free downloads from the Internet site. Unfortunately, from my point of view, the courses are not the familiar PGA tour courses. The sample software that was furnished has twenty additional courses, some were familiar from the tour events, and some are remakes of courses from previous versions. One of the courses common to both the new and old program editions is a Palm Desert, Calif. course: Bighorn Canyons Course.

The graphics in the older editions used mo-



saic-type pictures that do not look real. The new edition, for the same course, is imaged with small enough components to look more like a photograph. I can see why the programmers developed their own courses.

The Robert Trent Jones Capitol Hill Course, titled "The Judge," is in Montgomery, Ala. on the Alabama River. It one of the featured courses. The scenery is quite realistic. The area we see is that which is visible as you drive along I-65 from Birmingham. The first hole is shown from a photo but is recognizable from the scenery graphics.

Playing a Course

The setup introduces a "real time swing" where the player's arms move with the mouse. I found it hard to control but the movement of the entire forearm is supposed to translate into a realistic swing. Apparently, one late *Tiger Woods Golf* game uses a similar real time swing.

There is a "Classic" configuration where mouse clicks control a pallet and the player's action respond to the arc of the pallet edge tracer. This is how most of the earlier games worked and was easy to use. The pre-shot procedure also allows aiming the ball. This was easy to use in this edition because the line of



site view of the tee to green was augmented by a view where you could aim the ball. In challenge matches, this probably has to be turned off.

The shot setup, pre-shot and swing opportunities are repeated for each stroke the player makes toward the hole. The course setups in this latest version seem somewhat easier than previous versions if the "help" screens are used. The putting aim and distance aid significantly improved my scores on the courses that I played. It was easy to shoot par on "The Judge." In real life I could not hit balls the distances I was covering with the computer course shots.

Review Summary

1. The classic swing play is similar to other golf games and is easily mastered; the real time swing is more difficult.

2. The play can be mastered easily and is setup for various levels of challenge.

3. The scenery graph-

ics are photo recognizable, an improvement from other editions and impressive.

4. There are settable sound bytes which are OK but not spectacular.

5. Game resources do not allow multitasking while operating as expected in a *Windows* program.

6. On line play is available with multiple partners.

7. APCD (Arnold Palmer Course Designer), an additional program, is included in the package. The instruction manual can be found on-line. This feature allows designing new golf courses. There are several offered for sale on-line.

Requires: Pentium 400 Mhz or faster; 390 MB on hard drive, 16 MB RAM, 3-D Video Card, *Windows* 2000/XP, mouse, speakers.

\$ 25

www.microsoft.com/games/links2003/home/default_2.asp See trial version

Spyware Ate My Processor!

Editorial

By Gil Hennon

Last month in the School Bell column I went out on a limb by remarking that spyware is “fast becoming the biggest threat to individual privacy and data security that computer owners have ever encountered.” A couple of folks took issue with my position. Viruses and worms had recently caused them a great deal of grief. As far as they are concerned, spyware isn’t even a contender.

I’m not backing down though. Without discounting the risks associated with viruses, Trojans, worms, bombs, runaway spam, and all the various other nasties, I still believe that spyware is moving up on the pack. Spybots are also becoming dangerous much faster than any other threat we have encountered. Just a year or so ago, individual users worried most about email attachments while network administrators fussed around with filters to stop worms. Most of us had learned (sometimes the hard way) to use anti-virus software to scan our disks and broadband connected users were finding out that a firewall was also necessary.. About the only other “security measures” many of us even knew about were those included in our browser settings to control cookies, Java, and ActiveX.

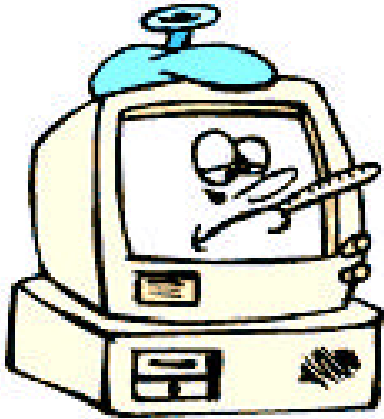
A seemingly helpful utility called Gator Wallet may have been the first to plant a spybot on user computers. Gator was a popular download on the freeware and shareware Web sites. It would jump in to help a user fill in names, addresses, passwords, and credit card numbers on forms. For quite a while, hardly anyone suspected that it was also harvesting information about the computer user and sending that information back to its home base. Gator, as well as most of the spyware that came along after it, is notorious for installing itself multiple times.

Many instances running simultaneously eventually consume enough processor time to make a user aware of their presence.

One reason that spyware didn’t draw much attention from users was intentional. Gator didn’t forcefully declare that its bot was being installed along with the visible utility. That gem of information was buried in the text of the software “license agreement.” Any user could read it before the installation, but few ever did. Some time later, Gator began to disclose up front that user data would be collected and how it would be used. Then it was up to the user whether or not to accept the deal. Other bot installers have been more or less open about what they are doing, but the majority of users were unaware of these harvesting programs running in the background until they caused some kind of problem. A lot of computers were already hosting a lot of bots before their existence became generally known.

Another factor contributing to the rapid increase in spyware is a more efficient and secretive delivery system. Rather than waiting for a computer user to download and install a program with an embedded bot, many Web sites can install the tiny programs on every computer that visits. Since it takes no longer to give a visitor a bot than to set a cookie, few users are aware that they leave with more than they expected.

Most spybots are simple, nearly benign small programs that pick up specific information, such as where a user goes on the Web, what products a user examines while on a Web site, or what a user wanted from a search engine. This information often feeds an online advertising process that delivers back a pop-up ad



that is hopefully relevant to the user's desires. Some bots bring back sales pitches that are neither relevant nor welcome. Pop-ups for online gambling, Viagra, pornography sites, and even less wholesome products now commonly assail computer users who never even went looking for such things. Bots are generating instant Spam that is more difficult to avoid or filter than the sort that comes in email. Bots also are indiscriminate in targeting users. Recently a Memphis teacher polled her elementary school students and found that more than half of them had seen pornographic pop-up advertising on a home or school computer.

The utilities that eliminate spyware have been around long enough to have matured into reliable and effective tools. *AdAware* from Lavasoft (www.lavasoft.de) was one of the first, and although it stagnated without any improvements for a couple of months earlier this year, it is now back up to speed and still the easiest to use. *Spybot Search & Destroy* (www.safer-networking.org/) also has an excellent reputation, although many users find it more complicated to use than *AdAware*. At least eight other "bot eliminators" are also available. Mike Healan's excellent Web site (www.spywareinfo.com) keeps track of new advances in anti-spyware software as well as providing a wealth of security and privacy information. He gives you the low-down on all anti-spyware utilities, and his weekly newsletter is really an eye-

opener!

It's curious that spyware and the software tools to eliminate it do not get much attention in computer magazines. Tech TV had a short spot about *AdAware* recently, but it is still surprising that many computer users have never heard of bots. When someone complains of poor performance from their PC, I always recommend downloading and running a spyware eliminator. It isn't unusual to find several hundred bots on a single machine. Once they are removed, the computer usually loads and runs programs several times faster. There are still lots of users completely unaware that they are hosting a bunch of bots, and this lack of recognition contributes to the proliferation of spyware.

I mentioned before that most spyware is relatively benign. Up until a couple of months ago, that was pretty much true. Spyware as it was originally implemented, a sub-category now called "data miner," still tracks a user's movements and interests on the Web in order to bring back advertising. Recently more malevolent and destructive bots have appeared that behave unethically, if not illegally. Some data miner bots go beyond the basic tracking functions and log a user's keystrokes. When this kind of information gets back to the bot's home site, it is filtered for username/password combinations, personal identification data, and possibly credit card account numbers. A recent bot collected login keystrokes from thousands of AOL members before it was identified and its home site shut down.

"Scumware" inserts ads or links on the Web pages of competitors, attempting to trick a customer away to another site. Usually the overlaid links are indistinguishable from other links on the page, and the destination is also in a similar style. Often the customer is unaware of having been taken somewhere else.

"Stealware" bots ought to be illegal, even though a judge has ruled that they

are not. This bot intercepts cookie information, making a destination Web site believe that a customer came there from the stealware's site, and not from the site that really provided the referral. This credits the owner of the stealware bot with any "click-through" cash the destination might pay. Since many non-profit and small sites survive on the funds generated by "click-through" traffic to vendors like Amazon, stealware bots harm innocent and worthwhile sites, eventually forcing them off of the Web.

A newer crop of nasty bots are "hijackers." As the name implies, they have methods of taking over some functions of a computer. A browser hijacker can force a user to a specific Web site rather than where he/she intended to go. Sometimes the hijacker inserts its own server address into the DNS fields of a computer's network configuration. Another method is to put entries in the computer's HOSTS file. HOSTS is the first place a computer looks when attempting to connect to a site. If the URL is in the HOSTS file, the computer connects to the IP address given by HOSTS. If the URL is not there, then the computer attempts to get the IP address from a name server on the Internet. By putting a bogus IP address for www.google.com in the HOSTS file, the bot forces the browser to go to the wrong site every time the user wants to go to Google.

The more sophisticated hijack bots will make Registry entries that change the DNS address or HOSTS file during each boot up. If you discovered that you were hijacked and put things right, your corrections last only until the next start. One of the recent hijack bots corrupts the Google add-on toolbar for Internet Explorer, sending any search keywords entered to a search site that links only to a select group of vendors.

The most common way to get a hijack bot is to respond to spam email. A link in

the email accesses a site that secretly installs the bot while displaying pop-up ads to keep the user occupied and unaware that something more sinister is going on. Getting rid of hijack bots can be a complicated manual process too, since only few of them are recognized and cleaned by standard anti-spyware software. If you suspect your browser has been hijacked, and ordinary attempts to fix the problem fail, go to tomcoyote.org and download the *Hijack This* tool. It makes a text listing from your Registry of all programs that start automatically. If you know what ought to be there, you can examine the listing and determine which lines should be removed and check the appropriate *Hijack This* boxes to perform the fix. Suspicious entries will contain terms like searchbar, toolbar, hotsearchbox, coolwebsearch, or mysearch. If you aren't sure what to tell the tool to remove, then post your listing to the *Hijack This* forum on tomcoyote.org and their wizards will tell you which bots hijacked your browser and how to get rid of them.

One spyware distributor insists its bot is not spyware, but actually a worthwhile addition to anyone's computer. *NewDotNet* adds the capability to access several unofficial top-level domains. (Top-level domains are the last part of a URL's "dot" address, such as COM, ORG, NET, and GOV.) *NewDotNet* enables dot SHOP, INC, FAMILY, CLUB, SPORT, and several other domains that, coincidentally, are all marketed by *NewDotNet*. Their bot steers communication with these domains to their DNS server because the regular crop of DNS servers, which adhere to official domains, are not able to resolve *NewDotNet*'s non-standard URLs. At first glance, that's not such a bad thing. Where the problem arises is that *NewDotNet* installs this bot secretly on computers of unsuspecting users when they download software of a completely different kind. So

NewDotNet enters a computer just like a Trojan Horse program. Once it is installed, it makes changes to the Winsock file, effectively corrupting it into a non-standard version of Winsock. This causes problems for other programs that expect Winsock to operate in the accepted standard manner. More than a half-dozen applications that have compatibility problems with *NewDotNet* are documented on various Windows User Help Web sites. *Norton Anti-Virus*, *ZoneAlarm*, and Microsoft's Internet Security functions have all experienced problems with the modified Winsock.

If you visit *NewDotNet*'s Web site, they seem to assume you are trying to remove their software, and offer several complicated methods for doing that if their uninstall utility failed to do its job. Strangely, the site says everyone is prohibited from distributing the uninstall instructions, mirroring them on another site, or even linking to them. Since I don't want to get MPCUG into any lawsuits, I'm not putting a link here. You'll have to add your own www and com around their name to get there. The site also warns visitors not to believe information about *NewDotNet* that may be found on other Web sites. While the *NewDotNet* Web site is carefully written and sounds helpful and friendly, there is an aura of arrogance and intelligence insulting rudeness in the site's attitude toward the user.

Maybe you need access to these unofficial domains. If so, and if you are willing to put up with some incompatibility with other programs, then you will find *NewDotNet* useful. I didn't, nor did I appreciate it being secretly installed on my computer. I got rid of it as soon as I was aware of it. By the way, don't try to uninstall it by simply deleting the files in the *NewDotNet* folder. That leaves you with a corrupt Winsock that can no longer connect to the Internet. *AdAware*, running the latest reference files, will remove it

safely and restore Winsock correctly. For doing that, *AdAware* is being sued by *NewDotNet*. Guess who I hope comes out a winner!

A spyware bot identified very recently also has the strangest purpose. I predict that *Lover Spy* will become a favorite of divorce lawyers and those who stalk others with a criminal intent. Once it is installed on a spouse, relative, employer, or complete stranger's computer, *Lover Spy* will record all email, chat sessions, Web site visits, keystrokes, and passwords processed by the target computer. It will also take "screen shots" of applications and opened windows. All of this is emailed to the person who orchestrated *Lover Spy*'s installation.

Aha, you say! That's the hard part, isn't it? How does one get someone else to install *Lover Spy* on their computer? Well, *Lover Spy* has a "false front" Web site with a selection of email greeting cards. They will send the person you target an email telling them that there is a greeting card waiting for them. When they go to the site to see their card, they are told that they need to install a plug-in before it will view it properly. The plug-in is the spyware program, and the victim consents to its installation. The victim does get to see a nice greeting card too, but that's beside the point. Whether or not this kind of "spy service" is legal or not will probably depend on a court decision.

So I still say that spyware will very soon be a greater threat to computer security than spam, worms, and viruses. That's my story and I'm sticking with it. I also wonder how long we have before we are running so many different security programs—anti-virus, anti-spyware, firewall, and intrusion detection—that our computers become useless for doing any real work. By all means, take care and know what your computer is doing when it thinks you aren't watching.

-0-

Microsoft Intellimouse Optical

Hardware Review

Reviewed by Rick Fischer

Pointing devices continue to evolve (slowly). My first was a large track ball in the P-3C Orion airplane in 1972. There was a joystick in the Royal Air Force Nimrod. My first mouse was a Microsoft ball mouse. I was impressed.

That gave way to the wheel mouse. Then the optical mouse – look, Mom, no ball to clean. It was smooth and although I was told I didn't need a mouse pad, I still use one. Most recently I tried the Intellimouse Optical. It has two programmable buttons on the sides which for me became “copy” and “paste.” There are 43 possibilities, e.g., cut, delete, double-click, forward or backward, F-keys, print screen.

It feels natural in my large hands. I am right handed. It is designed to feel natural for right and left-handed users. When I use someone else's mouse I find myself trying to press the two programmable buttons, whether they are there or not. It has become a natural extension of how I work.

The Intellimouse comes with its own software (on CD). You load the software. Turn off the computer. Replace your old mouse with the new one. Restart your computer. Then pro-



continued >>>

Memphis PC Users Group Membership Application

Date: ___/___/___

Membership # ___

Name: (Last) _____ (First) _____

(M.I.) _____

Mailing Address: _____ Birth Date: ___/___/___

City: _____ State: _____ Zip: _____ - _____

Home Phone: (____) _____ Business Phone: (____) _____

Fax Number: (____) _____ E-mail: _____

Employer: _____ Position: _____

Dues: \$35 per year

For office use only

Check#: _____ Amount: _____ Date: ___/___/___ Initials: _____

gram your two side buttons. If you don't like the choices you start with, you can easily change the settings.

After that, you just forget about and just get work done. That's what it's all about.

Requires: Win 98, ME, NT 4.0 with service pack 6 or later, Win 2000 Pro or XP. Pentium 133 Mhz or faster with Win 98 & 32 MB RAM. For XP, 233 Mhz and 12 MB RAM. CD-ROM drive. Microsoft Internet Explorer 4.01 with Service Pack 2 or later. Also works with a Macintosh.

Works with PS/2 and USB connections.

\$ 25

www.mirrosoft.com/mouse

***“If you
decide you
want ham in
your omelet after it
is made, you have
limited options.”
- unknown***

Out for Review

Here is a list of software, books, or other products you can expect to see reviewed here in the coming months. These members checked out items to review for the benefit of all.

Windows Me: The Missing Manual	Greg Adams
Teach Yourself GoLive 5 in 24 Hours	Allison Banks
Spell Catcher	Deborah Hart-Curtis
Civilization: Call to Power	Morgan Curtis
Microsoft Office 2000 8 in 1	Dorothy Drum
Windows Security Handbook	Dorothy Drum
The Little Web Cam Book	Mike Heinrich
Microsoft Works 7.0	Jim Ingram
How to Use Microsoft FrontPage 2002	David Levine
The Complete Idiot's Guide to Starting A Business Online	David Levine
Space Bunnies Must Die (game)	Adam Locke
Sin (game)	Adam Locke
X-Wing vs Tie Fighter	Adam Locke
Star Wars: Behind the Magic	Adam Locke
Extreme Tennis	Adam Locke
Photoshop Type Effects	Bill Luber
User Interface in C#	Jim McGee
Sportsman's Challenge	Kim McNeil
Top Shot	Paul Merz
Using MS Windows 2000 Prof	Eric Miles
FrontPage for Win 2000 (book)	Lee Mouring
Digital Video Pocket Guide	Vanessa Muldrow
Google Pocket Guide	Vanessa Muldrow
Windows XP Pro (book)	Daniel Notowitz
FrontPage 2002 Unleashed	Carl Osborne
Macromedia (book)	David Stowell
QuarkXPress 6 (book)	George Stringham
Windows XP (book)	Terry Thomas
eBay Hacks	Tommy Towery

Thanks to all who checked out products for review. Let's keep the Group vital and provide value for membership.

Linux Server Hacks

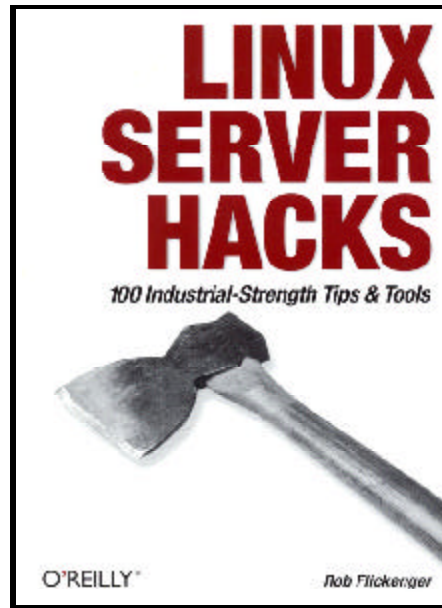
Book Review

by Gil Hennon

Imagine ordering a roast beef special in an unfamiliar restaurant. It isn't a fancy place. It has checkered tablecloths and the reasonably priced menu is written on a big chalkboard on the wall. There are no chandeliers or candles, and the servers aren't talkative, but they get things done quickly without any fuss. When your meal arrives, it is a generous, lean portion of prime rib cooked just the way you like it. Okay. I agree that it doesn't happen often. But when it does, it's a delightful surprise.

That's the sort of surprise you'll get from Linux Server Hacks. There's nothing fancy here. No fat. Just a couple of hundred pages of lean, useful tips for getting the most performance and productivity out of a Linux server.

I thought I knew quite a bit about Linux servers. I've set up six from scratch in the past year. This book was both humbling and enlightening. It reminded me that it is only by learning a lot about a subject that one finds out how



much more there is to know!

Like the prime rib, Linux Server Hacks is lean. It assumes the reader has already mastered Linux basics. Commands and syntax are not explained. Those can be found in the MAN pages anyway. Most of the hacks require entry from the command line, since GUI interfaces rarely support all of the switches and options that a system command can use. Don't let that scare you away though. Just expect to use another Linux book for basic information. This book will take up where that one leaves off.

It also helps to be at the keyboard rather than in an easy chair while

reading Linux Server Hacks. Performing the steps of many hacks in the book will help in understanding the purpose and how the tip will help. I'm sure some folks are capable of reading the book from cover-to-cover, but I found I understood lots of tips much better by using a hands-on approach.

One of my measures of worth for an instructional book is how quickly I find information that is immediately useful to me. Linux Server Hacks blew me away in the first chapter! Getting into performance issues right away, Rob Flickenger, the author, tells what shouldn't be running on a Linux server. There are about twenty optional services that start by default during the boot. A server that needs all of these is rare. Rob tells what they do—and I knew about less than half of them—and tells why you might or might not ever use them. Then he guides you through shutting each down and removing it from the boot process. The result is a faster running, more efficient Linux server that is not wasting processor cycles and memory on an unneeded service. That

was the first hack!

The rest of the book groups various hacks into related areas such as networking, scripting, etc. so it is easy to find a particular tip when it is needed. The first twenty or so hacks are grouped into a section called "Server Basics," but don't let the name fool you. These hacks are more like a graduate degree. Some are fairly simple, where perhaps only a parameter change in a standard command makes that command much more useful or provides more information. Some of the hacks require the reader to write a short script and then run it in the shell. In these cases, the script can be copied from the book into a file and there is a short tutorial or sample run to show how it is used.

A few hacks are complicated enough that a program or script should be downloaded from a third party. Along with instructions for downloading, Rob provides a brief description of the tool and usually a sample listing showing it being used. He sticks to his tendency for brevity with some of these, so pay attention. He will get you started, but will let you have the fun of discovering some of the tool's uses

for yourself.

My copy of Linux Server Hacks has several paper clips sticking out of it. I've marked hacks that I have tried on one or two servers and found the result to be especially useful. These I will also perform on other servers when I am doing maintenance. Some of the hacks I've liked will not apply to all of our Linux servers. They perform different functions, such as Web server, file/print server, and development server, so each gets some hacks that are relevant only to that server's function.

I would recommend Linux Server Hacks to anyone who is or wants to be a Linux administrator. If you are new to that position, you will become good at it much faster with this book. Experienced administrators will already know some of the hacks, but I'll bet that they still find plenty of tips they haven't used before. It is a book I will keep on the shelf beside my workstation.

Linux Server Hacks: 100 Industrial-Strength Tips & Tools by Rob Flickenger is published by O'Reilly & Associates, Inc. List price \$24.95 FRN. Get an MPCUG member discount by purchasing at www.oreilly.com.

Please Help

The MPCUG receives requests from local organizations looking for used computers and printers that individuals are willing to donate. We get requests from churches, schools, communities, and charities.

If you have an old Pentium 300MHz or higher in operating condition or a working laser/ink jet printer that you no longer use and are willing to donate, we will try to match you with a recipient in need of equipment.

Currently we have requests from two churches and the Collierville Food Pantry.

Please notify

Gil Hennon
gil@ahls.us

or

Jim McGee
jim_mac@bellsouth.net



For up to the minute information and special updates
 be sure to check our Web site at:
www.mpcug.org

	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
SEP- OCT 2003	29	30	1	2	3	4 INTERNET HARDWARE CANCELLED
OCT 2003	6	7 DOT.NET	8	9 VISUAL STUDIO	10	11 WEB WRITERS MS OFFICE
OCT 2003	13	14	15	16	17	18
OCT 2003	20 WORDPERFECT	21	22 MAIN MEETING	23	24	25 INVESTMENTS
OCT-- NOV 2003	27 CLIPPER	28	29	30	31 	1 INTERNET HARDWARE
NOV 2003	3	4 DOT.NET	5	6	7	8 WEB WRITERS MS OFFICE