Access

Newsletter of the Louisville Computer Society
Kentuckiana's Macintosh Users Group

August 2004

Firewalling 101

by Lee Larson

One of my favorite movie lines is from Star Wars. Obi-Wan, showing young Luke the spaceport at Mos Eisley says "You will never find a more wretched hive of scum and villainy. We must be cautious." That pretty much sums up a realistic attitude toward the Internet.

Soon after getting a cable modem, I noticed an appalling amount of traffic coming into the house, even when I wasn't doing anything. It turned out that almost all of it was from unknown people trying to break into my computers. Calling the traffic appalling, is no exaggeration — thousands of attempts per day — hundreds per hour. It continues today. During the last hour, there have been 62 attempts to pry open port 80, the Web server, and many other attacks on other ports such as ftp, ssh and sendmail. If every full-time Internet connection gets this much attention — and I suspect most do — imagine all the wasted bandwidth.

Mac OS X is immune to almost all these attacks because they're trying to exploit well-known Windows problems. Even so, it isn't good to complacently sit back and smugly assume your Mac is completely safe. All during the spring and early summer a steady stream of Mac security problems have been dribbling into the news. Even though Apple has been pretty good about releasing security updates to address these problems, there are still a few simple things you can do to make things more airtight. I'll bring up three of them here.

Most important and easiest, of course, is to make sure Software Update automatically checks for Apple's security patches. Set it to check every day, because an extra day with an unpatched hole is far too long to let the script kiddies pound away at your system.

The other two simple fixes take advantage of the Unix that lives under the hood of your Mac.

Two programs that control networking down in the bowels of Mac OS X are called ipfw and xinetd. The first is a geekish abbreviation for Internet protocol firewall and the second is the Internet control daemon. They're very subtle and powerful programs with hundreds of recondite options that let you control network access to the finest degree. There are whole books written about them. Fortunately, we only need to scratch the surface.

Apple has been nice enough to provide a simple program to do a basic setup of ipfw. It's the Firewall option in the Sharing system preference panel. Everybody should decide whether they want to allow outside machines to initiate connections with their local machine and how outside machines will be allowed to connect. Check the boxes for the services you want to share with the universe, and start the firewall. Only connections through those services will be allowed. Apple's built-in firewall is a pretty blunt instrument for controlling access. It's all or nothing for each service. For example, suppose you want to log into your home machine from your office machine while denying all others any access. This is easy to do with xinetd, but Apple doesn't provide an easy program to set it up and gives almost no documentation. To do so, you have to use the dreaded terminal and any text editor you want.

When a machine contacts your machine asking for a service, xinetd looks for two text files in the /etc directory: hosts.deny and hosts.allow. These two files can be used to tell xinetd what to do, right down to the machine level. It's easiest to understand what's going on by looking at a few examples. Here's my hosts.deny file.

```
all : all
```

That's the whole thing! All it does is deny all services to all machines. Here's a slightly simplified version of my hosts.allow file.

```
all : 127.0.0.1
192.168.0.0/255.255.255.0
136.165.6.167
```

This says that only three classes of machines can connect to all services. First is the machine with IP address 127.0.0.1. This is called the loopback address of the local machine and allows that machine can connect to all its own services. The second group, defined by 192.168.0.0/255.255.255.0 is just the machines in my house at home.

Firewalling...Con't on page 2

Louisville Computer Society, Inc.
P. O. Box 9021, Louisville KY 40209-9021

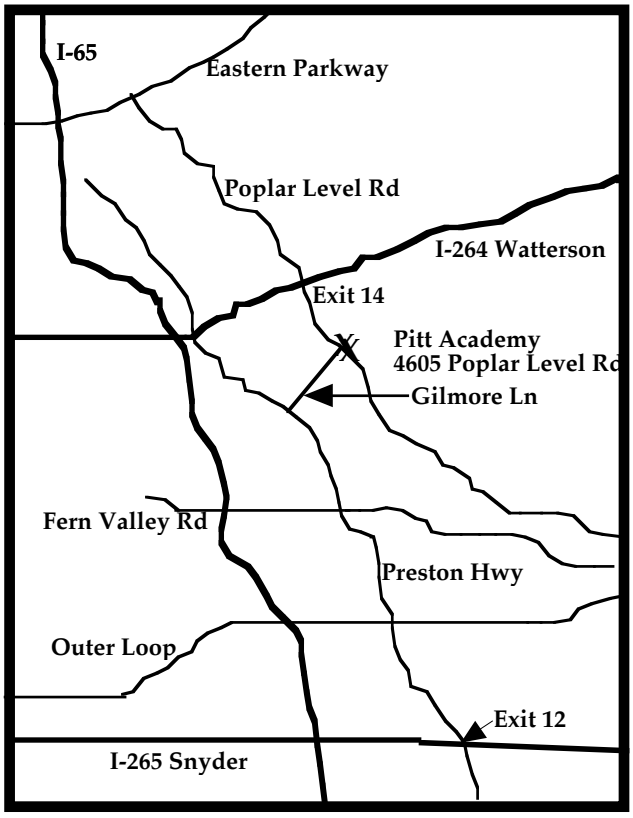
Access is a service mark of the Louisville Computer Society, Inc. Our newsletter is publisher monthly as a service to Macintosh users. We are dedicated to the education and benefit of Louisville and southern Indiana computer-oriented communities.

Subscription rate is $26 a year; it is mailed free with your membership in LCS, a Macintosh Users Group (MUG).

Come to our monthly meetings

The Louisville Computer Society meets the 4th Tuesday of each month, 7-9 P.M. (except December) at Pitt Academy, 4605 Poplar Level Rd. (Poplar Level Rd. at Gilmore Lane), Louisville KY 40213 (see map below).

Pitt Academy is 1 mile south of the Watterson on Poplar Level Rd. If coming from the Snyder Freeway, Gilmore Ln is 5 miles north of I-265 on Preston Hwy. Turn right and when you get to the end (Poplar Level Rd), Pitt Academy is directly across the intersection.



Firewalling...Con't from page 1

It basically says that any machine with IP address of the form 192.168.0.*anything* can connect. The final one, 136.165.6.167, is the address of my office machine. So, only machines in my home or office are allowed to connect.

Here's what happens when a connection is requested. First, xinetd checks the hosts.allow file to see what access the machine is allowed. If it's explicitly allowed to connect, xinetd starts the login. If not, it passes on to the hosts.deny file, which always says to hang up. There are at least a zillion clever combinations of commands to fine tune ipfw and xinetd. A good way to learn about them is to go Googling. For example, quick searches on hosts.allow or ipfw bring up thousands of references with many examples showing how to handle the most demanding situations.

Apple Releases iPhoto Update
By A. David Cooper , MacDirectory Editor

This new update (8/6/04), iPhoto 4.0.3, comes on the heels of an update that was released just days ago, (iPhoto 4.0.2), so while we aren't getting any official word from Apple, it's safe to assume that something wasn't quite right with iPhoto 4.0.2. Nevertheless, Apple has released the rapid succession update, so all iPhoto addicts can remain happy.

What is new in iPhoto 4.0.3 This update addresses several issues with using multiple text rules in Smart Albums and it also eliminates some problems with creating iPhoto books in the German and Dutch languages. Additionally, 4.0.3 keeps users informed about new version of iPhoto that have become available.

TIME Magazine's TECH TIME: School Tech Specs August 2, 2004
10 must-have gadgets that will fit student budgets large or small
Apple 12-in. iBook

LCS e-mail address book

Andrew Arnold	a0arno01@athena.louisville.edu
Jim Bennett	bennettsmay29@earthlink.net
Anne Cartwright	cartwrig@aye.net
Marta Edie	mledie@insightbb.com
Bernard Griffis	latigopc@bellsouth.net
Tom Guenthner	Tom@aye.net
Nelson Helm	helmkyny@clockwinders.net
Glenn Hoehler	glenn@insightbb.com
Harry Jacobson-Beyer	harryjb@bellsouth.net
Bill King	bk0413@insightbb.com
Lee Larson	leelarson@mac.com
Jeanne Montgomery	jerryandjeanne@aol.com
Tymna Oberhausen	tymna@bellsouth.net
Brian O'Neal	brimac@mac.com
Ed Stivers	stivers1@earthlink.net
Jan Weber	kyjweber@mac.com
George Yankey	jeffco13@bellsouth.net

If you wish to be added, contact cartwrig@aye.net

TIME MAGAZINE's GADGET OF THE WEEK
July 28,2004

Apple 4th-Generation iPod

Since the last issue, when I put in a bit about the iPod and it's "wheels," Apple unveiled its next-generation iPods 7/26/04). The new units are slightly thinner than the previous models and offer a 50% boost in battery life. The most notable change is the addition of the Apple Click Wheel, an innovation borrowed from the iPod mini. The buttons for Back, Forward and Pause/Play are now incorporated into the wheel, so without lifting your thumb, you can easily choose a playlist, scroll through songs and select one to play. Other enhancements include ability to make multiple on-the-go playlists, delete songs from on-the-go playlists and vary the speed of audiobooks. You can also sync and charge the iPod with either USB 2.0 or FireWire. The iPod is available in two configurations: 20GB for $299, and 40GB with the iPod Dock for $399.

iPod therefore I translate

<http://www.talkingpanda.com/>

Talking Panda sets a new standard for language translation software. Designed for the iPod, it's stocked with over three hundred essential words and phrases of the language you want to speak, organized for instant access. Download and install the program right now and begin your adventure abroad. Virtual fluency available in French, Spanish, and Japanese for $10 per language.

LCS Web Page, List Serve & Officers

Web Page	www.kymac.org
List Serve	macgroup@erdos.math.louisville.edu
Tom Guenthner, President	Tom@aye.net
Lee Larson, Vice President	leelarson@mac.com
Harry Jacobson-Beyer, Program Director	harryjb@bellsouth.net
Brian O'Neal, Web Master	brimac@mac.com
Anne Cartwright, Newsletter Editor	cartwrig@aye.net

What to do with an old Mac?

G4 Cube Aquarium
<http://home.comcast.net/~jleblanc77/cube/>

Blue and White Monitot terrarium for a Monitor Lizard?
<http://terrarium.geekvoice.net/>

Upcoming Programs 7 P. M. at Pitt Academy (see map on page 2)

August 24 **Harry Jacobson-Beyer and Bill Rising** with present an Applescript demo

September 28 **?????**

October 26 **Bryon Songer**, Apple's System Engineer, K-12 for Kentucky.

Future programs? What would you like to have??

Louisville Computer Society
Macintosh Users Group
Membership Application

Please send your $26 check for a year's membership, made out to Louisville Computer Society to:

Louisville Computer Society
P.O.Box 9021
Louisville,KY 40209-9021.

Thanks! See you at the next meeting.

Fill out the following ; clip on the dotted line (or copy to another piece of paper) and send in with your check .

❑ **New or** ❑ **Renewal Membership**

Name: _____

Home Address: _____

City: _____ **State:** _____ **Zip+4:** _____

Home Phone: ( ) _____ **Your E-Mail:** _____ **Your Home Page:** _____

How did you hear about LCS? _____

Apple's Firsts

1977 - The Apple II was not a "first," but the Apple II was the first "computer for the rest of us." It was the first mass produced COLOR computer. The computer remained on Apple's price list until 1980, and was followed by the Apple II/III Plus, Apple IIe, Apple IIc, Apple IIe Enhanced, and later the Apple IIgs which finally left the price list in the late 1980s!

1979 - VisiCalc, the first spreadsheet program, released for the Apple II -- marking perhaps the first time a software product drove hardware sales.

1983 - Lisa (forerunner to Macintosh), first personal computer with a Graphic User Interface

1984 - Macintosh released. First personal computer with dynamic memory allocation, API programming support (the Toolbox), a graphics API (QuickDraw), a global clipboard, Undo feature, and 3.5" floppy disk.

1985 - First personal computer with built-in networking (LocalTalk). Also, the LaserWriter establishes the Mac as the standard for desktop publishing, revolutionizing the print and publishing industry.

1986 - First personal computer with built-in SCSI (Mac Plus)

1987 - Plug-and-play expansion (Nubus in Mac II)

1987 - HyperCard introduces visual programming; MultiFinder brings multitasking (albeit not preemptive) to the Mac.

1988 - Plug and play SCSI CD-ROM

1988 - The first SuperDrive is introduced. Read/writes to Mac, DOS, OS/2, and ProDOS floppies.

1989 - 32-bit QuickDraw allows Macs to display photo-quality true-color images.

1991 -The first plug-and-play Ethernet networking cards

1991 - Apple petitions the FCC to allow personal computers to exchange information via wireless radio.

1991 - QuickTime, the first standard for dynamic media

1992 - WorldScript, the first worldwide language support for an operating system

1992 - The Duo is introduced with the DuoDock, code named BOB -- best of both worlds

1992 - QuickTime for Windows makes QuickTime the first cross-platform dynamic media standard.

1993 - ColorSync is the first color-matching technology built into an operating system.

1993 - First personal computers with built-in video digitizers and speech recognition (Quadra and Performa 660AV and 840AV).

1993 - Newton Message Pad introduced -- first handheld full-featured computer

1993 - First unified telephony and email architecture for a personal computer operating system (PowerTalk and PowerShare)

1993 - First personal computer with built-in TV and CD stereo system (Macintosh TV)

1994 - Power Macs debut, become the leading RISC-based personal computers.

1994 - System 7.1 for Power Macs is the first operating system to use emulation to run parts of itself, as well as legacy application software (i.e., the backward-support is done in software).

1994 - First 24-bit color digital camera under $1000 (QuickTake)

1994 - First next-generation typography engine (QuickDraw GX)

1994 - First panoramic virtual-reality technology for personal computers (QuickTime VR)

1995 - PowerBook 5300 was the first PowerPC notebook and the first to include a sleep-swappable drive bay. Included IR receiver for wireless networking.

1997 - PowerBook 3400 -- fastest portable computer in the world also utilized the 1MB IrDA Infra-red standard.

1997 - The 20th Anniversary Mac with integrated TV/Radio system, Bose sound, S-Video input

1997 - Power Mac G3 utilizes the PPC 750 Processor co-designed by IBM and Motorola, and was the first processor capable of using a "backside" cache, which could communicate directly with the processor at extremely high speeds.

1998 - The iMac is introduced. Unique in its lack of floppy drive, the iMac included a 4Mbps IrDA port and an internal 56Kpbs modem, used two 12 Mbps Universal Serial Ports (USB) as its only means of external expansion, and included a newly-designed USB keyboard and mouse.

Recent History - AirPort wireless 802.11b was brought to the mass market, Gigabit ethernet standard on personal computers, FireWire 400 and 800, the second coming of the SuperDrive (CD-RW,DVD-R), iSight, AirPort Extreme 802.11g, 64-bit processing, and a host of innovative software products, including the best and most solid operating system on the planet!

From Kibbles & Bytes #342
<Kibbles&Bytes@list.smalldog.com>

Louisville Computer Society
www.kymac.org
Macintosh Users Group
P. O. Box 9021
Louisville KY 40209-9021

37¢

Mailing Label