ASK KLAUS!

Klaus Knopper is the creator of Knoppix and co-founder of the LinuxTag expo. He currently works as a teacher, programmer, and consultant. If you have a configuration problem, or if you just want to learn more about how Linux works, send your questions to:

klaus@linux-magazine.com

Soundcards

I always read your articles, and I love Knoppix, I was curious about your answer in Febuary 2007 to a user having problems playing back audio from his DVDs. A common problem for any Linux distro is a computer in which the soundcard(s) cannot share the audio hardware ports. Mainly the onboard audio chipsets on most MBs cause this problem; they cannot share the ports due to hardware limitations.

I've found that soundcards for Linux installations need to have chipsets that can leave their ports open. Most soundcards that work on this level are Creative Labs, M-Audio, Turtle Beach, etc. Linux works great with these soundcards.

On a system in which the computer is using the onboard audio incorporated on the motherboard, the audio chipsets have limitations. Usually the Linux system sound server is running, and thus the ports are locked.

The only access to sound is through the Linux Sound Server (because it's running). Xine-based players default to Alsa or OSS, which can't access the cheap soundcard because the port is locked and not open.

Xmms will work using the arts plugin. It also depends on how the Linux system sound is accessing the card. The Linspire sound server system uses Jack, so programs using Jack will work with these limited soundcards (or arts). Anyway, onboard motherboard audio or a cheap audio card isn't the best hardware setup for a standard Linux distro.

The problem that you describe (the fact that a soundcard can just be "opened for write" by one program at a time) is more subtle. A "failed open" on */dev/dsp* or */dev/snd/pcm** indeed means that another process has that device open.

The most "apparent" solution would be just allowing the sound driver concurrent "open" accesses. However, there is a reason for locking the sound device exclusively for one program, and that has to do with the way sound output works.

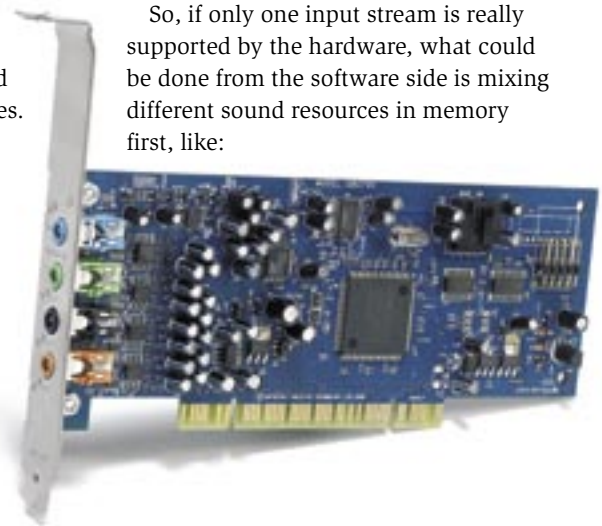
You cannot just write a wave or MP3 file to the sound hardware directly, like you would do on a tape or printer device. The way it works is that sound data is being stored into memory, and the address is sent to the soundchip DMA controller, so it plays a certain amount of sound at a time, from the given start to the given end address.

Some cards have an internal buffer for sound, so you can send a limited amount of sound data to that buffer first, which is then played by the card.

This method is usually used for storing instrument patches or fast effect sounds. More expensive soundcards may support multiple buffers or DMA channels that are first filled and then mixed, at once, using the soundcard's own mechanics. The usual sound hardware has one stream that is supported at a time, so naturally most sound drivers are designed to lock the software-side port, the sound device file, once the card is playing a sound.

If you would really be able to write concurrent sound data to the same address, the result would not sound similar to any of these two sound streams. In the best case, you would get some random noise. In the worst case, it will be really loud noise.

So, if only one input stream is really supported by the hardware, what could be done from the software side is mixing different sound resources in memory first, like:



```
sound_out = ➥
( sound_1 + sound_2 ) / 2
```

and sending the result to the card. Or a different plan would be to create a queue, like you have for sending print jobs to the printer, and play each sound after the other.

This can be important if you don't want to lose any information that can be given with sound, like in text-to-speech. There is even a "speech-dispatcher" available with a scheme that allows you to interrupt spoken text with more important spoken text and continue with the old text later.

One or both of these approaches are what sound servers like artsd and esd are supposed to do. But once they are running, the sound device is completely blocked for other programs until the server releases the device; it is not a good solution when there are programs that are not aware of sound servers.

To find the process that is guilty of blocking your soundcard, you can use:

```
fuser -v /dev/dsp
```

(*/dev/dsp* is, in the ALSA driver case, the OSS-compatible device when the *snd-oss-pcm* module is active).

Some of the ALSA drivers are capable of (almost) realtime mixing of different sound resources. This allows seemingly concurrent and parallel access to the sound device and "blended" sound output.

There is a (built-in) plugin, dmix, for ALSA that does this. The dmix setup is a little more complex and also depends on the type of card used.

More information on how to set up dmix is on the ALSA unofficial wiki at: *http://alsa.opensrc.org/index.php?title=DmixPlugin*.

Desperation

Can you help me please? I am desperate. I want to escape the clutches of Microsoft and recently loaded Linux Ubuntu from the CD that came with your magazine. However, how does one use Linux? There is no help or manual that I can find.

I want to access the Internet. How does one do this? How does one set up the modem, etc.? I cannot find any way to do this in the menus.

Every time Linux boots up it asks for a password. This is obviously most annoying.

Can it be set up not to ask for this password?

And what happens if you lose the password? How is a user able to get into the system without have to reformat the HDD and then reloading Ubuntu?

I do get a lot of email asking me to explain all of modern computer technology in just a few sentences that will be easy for beginners to understand, but this is unfortunately not possible. I'm just a computer user, too, and I have to look up information every now and then myself. The Internet is a good source of information on Linux.

Figure 1: Enabling password-free login in Ubuntu.

Ubuntu provides online help in several forms. See page 19 of the magazine in which you got the DVD for a summary of support sites.

The first thing to understand when you are learning to find your way around Linux is that "Linux" is a *computer operating system*, which is something most users don't "use" directly.

More often, you will probably be using an application, like OpenOffice for writing documents, GIMP for professional photo postprocessing, or Firefox and Thunderbird for accessing services on the Internet.

Be as specific as you can about what application you actually need help with before going to books and online help sources. Keep your focus on knowing what you want to do with the computer as a tool, rather than learning the technical details of how a computer works. The specific details are not really that important unless you happen to be interested in them.

When you are watching TV, for instance, you probably don't want to know what kind of electrical components are inside and what they are doing. (Of course, some people do find that kind of thing extremely interesting.)

You have to decide first what you want to do, then choose from the many possible tools for accomplishing that goal. I would need to know more about your modem to help you configure it.

A good starting point is the Linux Modem-HOWTO, which is available through the Linux Documentation Project (*http://tldp.org/HOWTO/Modem-HOWTO.html*). Check Ubuntu sites for Ubuntu-specific information.

Yes, it is possible to configure your Linux system so you can log in without a password. Every distribution has a way to do this.

You don't mention which version of Ubuntu you are using.

In Ubuntu 6.06 "Dapper Drake" you can select *System* in the main window and choose *Login Window*. You'll then have to provide a password to access administrative functions.

In the *Login Window* dialog, you will select the *Security* tab and check *Enable Automatic Login* (see Figure 1). Make sure your account is selected in the *User* box. Next, click *Close* to close the *Login Window* dialog.

You can still make your system usable again if you lost or forgot all passwords, provided you have physical access to the storage media and you did not encrypt the data.

This type of troubleshooting is an important reason for live CDs such as Knoppix. (The April 2007 issue of *Linux Magazine* includes a Knoppix DVD.)

It is even possible to use a Linux system for rescuing data from and repairing Windows installations, but again, the details will depend upon your situation. Users who are considering a change

from Windows to Linux may be interested in a document titled "Linux Is Not Windows," by Dominic Humphries: *http://linux.oneandoneis2.org/LNW.htm*.

DHCP Woes

I have broadband with Optus in Australia. Optus provided me with a Siemens modem with pppoe built in. I originally set it up with Windows. Most live CD and DVD distros wouldn't connect, however, Gentoo 2006.1 did. The difference seems to be that it uses dhcpcd rather tham pump or dhclient.

I have since tried several 2.6 live CDs, and if I mount my Gentoo partition and invoke its dhcpcd *./dhcpcd -h `hostname`*, they will connect. pump or dhclient must be stopped first, of course.

Is there a way to get pump or dhclient to work since dhcpcd is working? The modem has upnp enabled.

You could try some of the settings mentioned in the pump manpage. Unfortunately, there does not seem to be a specific program that always works best. In some cases, pump does fetch IP addresses when dhclient or dhcpcd fail. pump may require some cards to be activated with the command *ifconfig eth0 0.0.0.0 up* (replace eth0 is the actual device name).

You may also want to experiment with some settings in */etc/pump.conf*:

```
# Number of retries
retries 16

# Giving up after this time
timeout 60

# Skip nameserver (if running ➥
a local cache with a fixed ➥
/etc/resolv.conf entry)
nodns
nonisdomain
```

Malware Attacks

Why is it so hard to find articles about security in Linux? Is Linux free from spyware, viruses, and malware attacks? If not, how do I protect my system? Is there a scan package available, at least for spyware?

Figure 2: The Common Vulnerabilities and Exposures Project (CVE) provides updates on recently discovered exploits.

It's not too hard to find information about Linux security, or rather, Free and Open Source software security. There are many security portals and "Bug of the month" mailing lists, for virtually every part of Linux. GNU/Linux, like any complex system, is not free of errors or bugs, security flaws, and possibilities for circumventing malformed security restrictions. But, because of its open source nature, bugs are found and eliminated quickly, and you don't have to wait for a "patch-day" to make your system secure again.

Viruses are very rare (if not even non-existent) in Linux because of the very strict privilege separation in Unix systems. Trojans and Worms usually need some kind of interaction with the system administrator in order to get installed, or at least they require very weak permission settings (like global write access to device files).

Some Worms try to exploit flaws like buffer overflows in software running with root permissions. But systems with a higher security level, like a restrictive SElinux setup, are even immune to that. (I would not say that it's impossible to break in, but it's at least very hard, even if you have a lot of knowledge about system internals and possible exploits.)

All in all, no operating system I know of is absolutely immune, but a well-known fact is that "Security by Obscurity" has never worked. The closed-source practice of keeping errors and information about weaknesses secret does not make an operating system secure. Secretiveness just puts crackers at an unfair advantage because they get to know break-in possibilities first, weeks prior to the system administrators who could have fixed the problem had it been published properly.

Check the security page for your Linux distro for periodic updates on security problems. (See the "Insecurity News" on page 16 for more on obtaining security updates for popular Linux variants.). You'll also find information on exploits at the Common Vulnerabilities and Exposures project at *http://cve.mitre.org/*.

A number of tools help system administrators check for potential problems and identify break-in attempts (even successful ones). I recommend Nessus (*http://www.nessus.org/*) for checking for open ports and vulnerable network services running on your computers, Tiger (*http://www.net.tamu.edu/network/tools/tiger.html*) or Tripwire (*http://www.tripwire.org*) for local security and file system integrity checks, and Snort (*http://www.snort.org*) as an intrusion watchdog.

Several virus-checking tools are available for Linux. One popular solution is the open-source ClamAV anti-virus toolkit. For more information, visit: *http://www.clamav.net/*. ■

Send your Linux questions to klaus@linux-magazine.com.


sxc.hu