Building a self-contained auto-configuring Linux system on an iso9660 filesystem

Klaus Knopper <*knoppix@knopper.net*>
http://www.knopper.net/knoppix/

Abstract

Bootable CD-Roms with a small Linux rescue system in business card size [1, 2] or regular size live demonstration CDs [3] are becoming popular recently. Also, some of the commercial Linux distributors as well as non-profit Open Source groups are developing self-running demos that are preconfigured for certain hardware, or contain a configuration frontend. *Knoppix* (Knopper's *nix) is an attempt to not only create a fully featured rescue/demo system on a single CD, but also to unburden the user from the task of hardware identification and configuration of drivers, devices and X11 for his or her specific hardware. The resulting product is supposed to be a platform CD with a stable GNU/Linux base system, that can be used to customize static installations for a specific purpose.

Goal: Creating a fully functional and usable Linux system running completely from a single CD

A frequently asked question asked by people who "just want to have a glance" on Linux to check out how useful it could be for them is, "How can I test Linux without having to change anything on my computer?". Another issue often requested by those already familiar with Linux is, that there is seldom a fully installed and configured Linux system in reach when you could need one for network debugging purposes or simple tasks like converting files from and into different formats, recover lost data from a corrupt file system or run software that simply only exists for Linux. A "portable Linux allround system", but without having to carry around a notebook or mobile computer which can be lost or damaged, wouldn't that be a great help?

Knoppix is a one-CD live filesystem that can be customized as rescue system, security scanner or platform for presentations and demos, or as full-featured portable production platform with tools like KOffice or StarOffice™.

The underlying GNU/Linux base system is modified to boot non-interactively into runlevel 5 with a working X-Window and KDE [6] configuration, with all auto-detectable devices configured, ready to (auto-)start applications.

Reducing space limitations by compression

The core system of about 200 MB (uncompressed) is currently based on the popular RedHat [4] distribution and contains all basic commands and tools for a generic Linux system. That leaves, on a standard 650 MB CD-Rom, over 400 MB for custom applications, which can simply be installed with standard RPM packages on the CD-Rom install/preparation system.

As of Version 1.2, *Knoppix* features a transparently decompressing loopback-blockdevice derived from Paul 'Rusty' Russel's `cloop` kernel module hack. For a standard Linux installation, this reduces the space needed on the CD to about 50% down to 25% of the original filesystem size and leaves more space to custom applications or multimedia datafiles. The compressed live-filesystem is therefore present as a single file on the CD which is being mounted via cloop from the bootfloppy or El Torito bootimage at system startup, from the ramdisk containing the root filesystem. For performance and stability reasons, iso9660 has also been chosen as the underlying filesystem for the compressed image instead of a read-only ext2 filesystem that is common on other live CD-Roms.

The compressed filesystem not only adds free space on the CD, but also reduces access time and head movement of the CD-Rom drive, but handles physical read errors more ungraciously than an uncompressed filesystem and increases production time of a new release, because the whole installation filesystem needs to be compressed before the new version can be burned and tested.

Platform and Applications

Knoppix provides a ready-to-run operating system environment to:

- start security and auditing tools like *nmap* [8], *nessus* [7], *dsniff* and alike. Since there is no permanent storage present on a read-only CD-Rom, no sensitive information can be written or exposed accidentially. The security checks can be performed on computers directly within a customers network by simply booting from the CD on a machine that is already connected to the internal network,
- produce game and application demos that run in a safe and tested environment,
- have a stable demo installation of GNU/Linux available for presentation at trade shows or consulting talks with customers,
- build a customized, read-only Linux installation for educational environment which is preconfigured for internet access and contains all commonly used applications for this purpose,
- present the features and use of GNU/Linux without having to go through a long and maybe complicated installation and configuration process,
- feature a complete rescue and crash recovery system for all kinds of emergency issues with all necessary filesystems in the kernel, and repair tools available.

Technical Details: Boot process, automatic hardware detection and configuration, autostart of X11 and applications

In stage 1 of the boot process, the Linux loader LILO from the boot section of the el torito [5] 1.44 MB floppy image on the CD-Rom tries to read the kernel (currently 2.2.16) and an 4 MB compressed initial ramdisk. The size of this initial ramdisk determines the minimal amount of memory needed to use the distribution.

Without XFree [9] and KDE, about 8-16 MB of RAM seem to be sufficient for a working textmode-only environment.

In stage 2, the boot ramdisk tries to autoprobe for the most common SCSI adapters and identifies the CD-Rom drive where the *Knoppix* CD is located. The minirootdisk features a statically linked shell with commands like `mount` built in, since the space on the bootfloppy is limited. For compatibility reasons with current floppy drives, only a 1.44 MB floppy image is used on the CD instead of a 2.88 MB. The boot script tries to find the

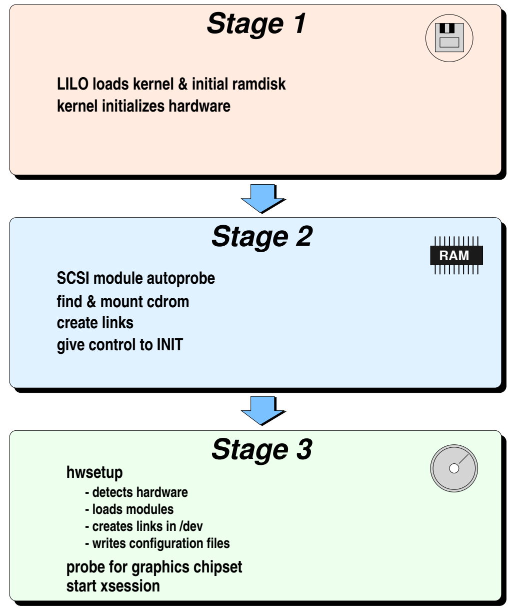

Figure 1: The boot process

Knoppix CD by mounting all CD-Rom drives and checking for a directory `KNOPPIX` that may contain a directory tree for the root filesystem or a file with the same name containing a compressed iso9660 image of the file system which is then mounted via the `cloop` device. If no CD is found, an attempt is made to find the `KNOPPIX` directory on an existing ext2 harddisk partition, containing a complete installation tree.

In either case, symbolic links are set to the uncompressed (or transparently decompressed) directory tree.

After the CD has been mounted, dynamic library cache and paths are initialized and space is freed on the root ramdisk by removing files that are no longer needed for the setup process.

If a swap partition is detected during device/partition scan, an attempt is made to utilize it via `swapon` to increase workspace for applications.

Also in this stage of the system startup, additional ramdisks are mounted with a writable ext2 filesystem for `/home` and `/var`. Their size is adapted from the available amount of real memory. Symbolic links to system directories are created and control is given to `init`.

In stage 3 of the boot process, `init` calls a finalizing setup script named `sysinit`. In this script, the automatic (or, if ”expert” mode was selected, manual) hardware setup is done. `hwsetup` - a selfmade tool that uses the `kudzu`-library [4] - detects devices, loads all necessary driver modules for known hardware, sets up symbolic links in `/dev` and writes configuration parameters and options to the corresponding files in `/etc/sysconfig/` on the ramdisk. Parameters that cannot be auto-detected (frequency ranges of old monitors, desired keyboard layout, language) are assumed with reasonable defaults. A single X-Window session is started if the graphics hardware has been identified correctly. Default is truecolor in a resolution of 1024x786 pixels if possible, or 800x600/640x480 at 8-bit if the graphics adapter cannot handle higher resolutions or color depths. If detected, the accelerated XFree (3.3) drivers are used with specific options depending on the detected graphics adapter.

The KDE Desktop manager (currently Version 2.0 beta 3 as of this writing) is started only if there is at least 30 MB of RAM left after all ramdisks are mounted and all necessary device drivers are loaded. Otherwise, a less memory-consuming windowmanager (like `twm`) is used, if XFree can be started at all.

Network device parameters can be set with a tiny `dialog`-based GUI from within KDE, if needed. For dialup Internet access, `kppp` or `isdn-config` [4] are provided.

Security issues

All user passwords, including the root password, are disabled and locked by default. That makes it impossible to log in via network or even on a local console. Therefore, all processes must descend from the shells running on the system console(s) or from the X-Window session that is spawned by `init`.

If the *Knoppix* user wants to enable a remote login, for example via the *openssh* daemon, she has the choice of adding a user with password, or generating an authentication RSA key for this user. There is no `inetd` meta daemon and no standalone servers running per default, that could be accessed from the network, if network is even configured.

A difficult issue is the local security and access to devices, because there is no reliable way to protect the switching from an unpriviledged user account to the system administrators id if passwords have been disabled. Having "dummy passwords" or default crypto keys that are written on every CD would of course breech security. In the current version, the automatically logged-in user at the system console is the system administrator. This can be changed in `inittab` and in the `xsession` init script at the preparation phase of a new CD-Rom image; for example, if the resulting system is supposed to work as a game or demo plattform rather than as recovery system or security scanner. Games, user-mode applications or demos should run fine with an unpriviledged account. In this user-only mode, runtime configuration of priviledged drivers, devices and configuration files is impossible.

Project status and distribution policy

The *Knoppix* CD currently contains the base linux system software plus utilities for a rescue system, current security scanners, demos and some of the KDE and Gnome games. It boots and auto-configures correctly on most ix86 comptible desktop machines. The most common PCI cards (network, sound, SCSI) are auto-detected, drivers are loaded and mice, modems, CD-Rom devices, CD-Writers etc. are given their appropriate links in the `/dev` directory. Harddisk partitions are detected and corresponding icons are added on the KDE desktop.

Most problem cases where the automatic hardware-detection fails have been Notebooks with new chipsets that are not supported by the current linux kernel yet.

In case of failure to correctly auto-detect and configure all necessary hardware components, the CD can be booted with an "expert" option for interactive setup.

The *Knoppix* base system (excluding vendor-specific add-ons which are separate products) is an Open Source project and covered by the GNU General Public License Version 2. The program sources of the software included is available from the vendors specified in the RPMs, the sources of the *Knoppix* setup tools or patches for programs needed to generate the automatic setup system can be found at [10], if not already present on the CD-Rom.

Because of legal issues (i.e. US crypto export regulations and software patents that may disrupt commercial and noncommercial use of software included on the CD, that is otherwise covered by a Free Software license, for example strong crypto versions of KDE or other SSL-enabled software), the author does not currently distribute the *Knoppix* CD publically. Individuals or companies can order a customized CD version for evaluation or software projects directly from the author.

Features in development and (previous) TODOs, sorted by priority

1. Use a transparently uncompressing block device to increase the space available for installed programs. *Status*: Done. Needs cleanup and more checks.
2. Disable spin-down of CD-Rom Drive for faster CD-Rom access after periods of idle time. *Status*: Still looking for a way that works vendor-independent.
3. Clean up boot disk (only 50 bytes or so left), make `insmod` a builtin function of the initial shell. *Status*: `insmod`, `rmmod` and other commands are now builin part of the initial shell. Most SCSI drivers of Kernel 2.2.16 fit on the 1.44 MB boot-floppy now.

4. Generate set-ups that are easily customized for different purposes rather than install and uninstall RPM packets before creating a new image. *Status*: Still working on a method to do this easily.

5. Enhance interactive setup for using existing swap partitions. *Status*: Existing and previously initialized swap partitions are now detected and utilized during the boot process.

6. Add session configuration that can be customized, which can be saved on removeable media. *Status*: Not done yet.

7. Enhance the auto-detection process, increase the number of known cards and recognized graphics adapters. *Status*: Used information retrieved from betatesters to create configurations for problematic hardware (mostly Laptop chipsets), ongoing process.

8. Add support for automatic, non-interactive setup of isapnp devices. *Status*: Not done yet.

References

[1] `http://www.innominate.de/`

[2] `http://www.linuxcare.com/`

[3] `http://www.demolinux.org/`

[4] `http://www.redhat.com/`

[5] `http://www.ptltd.com/products/specs-cdrom.pdf`

[6] `http://www.kde.org/`

[7] `http://www.nessus.org/`

[8] `http://www.nmap.org/`

[9] `http://www.xfree.org/`

[10] `http://www.knopper.net/knoppix/`

About the author:

Klaus Knopper holds a master's degree in electrical engineering and works as a consultant and programmer for Linux-based intranet/internet gateway solutions, firewalls and VPNs.