Argus Security Solutions for Linux

PitBull LX Installation Guide

Release 1.1.1
February 15, 2002

x86

Argus Systems Group, Inc.
1809 Woodfield Drive
Savoy, IL 61874

Installation Overview

The installation process requires the following steps, in order:

Pre-Installation

- ❑ Install and configure hardware and software.
- ❑ Review the documentation included on the CD.
- ❑ Review the documentation for configuring and compiling a Linux kernel.
- ❑ Review the documentation (man pages, info pages, etc.) for your bootloader (`lilo` or `grub`).
- ❑ Acquire license information and obtain license from Argus.

Installation

- ❑ Install PitBull LX.
- ❑ Compile and install a new kernel.
- ❑ Configure your bootloader to use the new kernel.
- ❑ Reboot the system.

Post-Installation

- ❑ Read the product documentation thoroughly.
- ❑ Configure PitBull LX.

It is possible to render the target system inoperable by making bad choices at critical times during the installation. Follow the instructions carefully.

After installation, read the product documentation thoroughly before attempting to implement the security features of this product.

Documentation on CD

All Argus documentation for this product is available in electronic format in the following directory on the installation CD-ROM:

```
<mount-point>/docs
```

Pre-Installation Information

System Requirements - Hardware

- ❑ Intel x86 (or compatible) system
- ❑ 32 megabytes of RAM
- ❑ 15 megabytes of additional space in the / partition
- ❑ 1 megabyte of free space in the `/boot` partition
- ❑ 1 megabyte of free space in the `/usr` partition
- ❑ 175 megabytes of free space in the `/usr/src` partition

System Requirements - Software / Setup

A Linux based system must be installed and configured prior to PitBull LX installation.

Automated installations that are currently supported are:

- ❑ Red Hat Linux version 7.1
- ❑ Red Hat Linux version 7.2
- ❑ SuSE Linux version 7.2
- ❑ SuSE Linux version 7.3
- ❑ Linux Mandrake version 8.0
- ❑ Linux Mandrake version 8.1

A generic installation procedure is available for other Linux distributions.

The tools required by your distribution for kernel compilation must also be installed. This will include a C compiler, assembler, make utilities, and `bzip2` compression utilities.

License Information

You will need the following information to obtain a license:

- ❑ Your company's name, address, and contact information
- ❑ Your machine's architecture (x86)
- ❑ Your machine's operating system
- ❑ Your machine's host name
- ❑ The Argus product you will install (PitBull LX for Linux)
- ❑ The number of processors on the machine

When you have this data, contact Argus Systems Group by email at license@argus-systems.com or by phone at (217) 355-6308.

Argus can send your license information to you via email, fax, or conventional mail; however, email is preferred. You will be asked for the Argus license data during installation.

Installation Procedure

Install PitBull LX

1. Read the Release Notes on the CD-ROM prior to installing the system. (`docs/RELEASE_NOTES.txt`)

2. Log into the system as `root`.

3. Mount the PitBull LX CD-ROM. Make sure the CD-ROM is not mounted with the `noexec` option. For example:

```
# mount -t iso9660 /dev/cdrom /mnt/cdrom
```

4. Change your working directory to the mount point of the PitBull LX CD-ROM. For example:

```
# cd /mnt/cdrom
```

5. Change your working directory to the directory containing the product for your specific distribution.

For example: If you install PitBull LX on a Red Hat version 7.2 system, you would

```
# cd redhat7.2
```

NOTE: If you are installing on a distribution that does not currently have installation support, you will need to enter the `generic` directory. Please see the `README` there for further instructions.

6. Run the installation script.

```
# ./install.sh
```


This script guides you through most of the installation process and installs the product. Where prompted, perform the following actions:

a. Agree to the terms of the software license agreement.
b. Choose which components are to be installed.
c. Enter license information obtained from Argus Systems Group.
d. Confirm requested information.

File Changes

The installation makes the following changes to existing files:

All Distributions:

`/sbin/e2fsck`	moved to `/sbin/e2fsck.orig`
`/sbin/e2fsck, /sbin/fsck.ext2, and /sbin/fsck.ext3`	replaced

Red Hat, Mandrake:

`/etc/rc.d/rc.sysinit`	moved to `/etc/rc.d/rc.sysinit.orig`
`/etc/rc.d/rc.sysinit`	replaced

SuSE:

`/etc/init.d/boot` moved to `/etc/init.d/boot.orig`

`/etc/init.d/boot` replaced

Configuring and Compiling the Kernel

Before using PitBull LX you need to compile the kernel source that was installed earlier. This section walks through the procedure.

1. Change your working directory to `/usr/src`.
2. Remove the `linux` symbolic link, if it exists.
3. Create a symbolic link from `linux-2.4.17-argus1` to `linux`.
4. Change your working directory to `linux`.
5. Remove any stale objects and configurations by using `make distclean`.
6. Configure the desired characteristics of the kernel by using `make config`, `make menuconfig`, or `make xconfig`.

In addition to the configuration options that you wish your kernel to have, you must enable the following options.

Select "Enable loadable module support," and "Kernel module loader" from the "Loadable module support" menu.

Select "ARGUS support" from the "General setup" menu.

You must also include support for your root device (i.e. SCSI adapter, IDE adapter, etc.) as "built in" (not a module).

Now create the proper dependencies with the following command:

```
# make dep
```

Build the compressed kernel image with:

```
#  make bzImage
```

Build the necessary kernel modules with:

```
#  make modules
```

Installing the New Kernel and Modules

To save the modules from a previous kernel, move the modules.

```
#  mv /lib/modules/2.4.17-argus1
            /lib/modules/2.4.17-argus1-old
```

Install the new modules.

```
#  make modules_install
```

Install the new kernel.

```
#  mv arch/i386/boot/bzImage
            /boot/vmlinuz-2.4.17-argus1
```

(Note: If you have a previous kernel with the same name, rename the previous kernel.)

Install the new System.map with

```
#  mv System.map /boot/System.map-2.4.17-argus1
```

(Note: If you have a previous mapfile with the same name, rename the previous mapfile.)

Configuring your bootloader

Your bootloader (`lilo` or `grub`) needs to be aware of your new kernel in order to boot it.

Configuring `lilo`

1. Open the file `/etc/lilo.conf` for editing.
2. Copy the currently used image entry, removing any `initrd` tags.

3. Edit the image tag to reflect the new kernel.

```
image=/boot/vmlinuz-2.4.17-argus1
```

4. Change the label tag to `argus`.

```
label=argus
```

5. Change the default tag, if present, to `argus`.

```
default=argus
```

6. Save and close the `/etc/lilo.conf` file.
7. Run the `/sbin/lilo` command to commit the changes.

Sample before and after `/etc/lilo.conf` files are shown below (bold type indicates changes):

Before:

```
boot=/dev/hda
map=/boot/map
prompt
default=linux
image=/boot/vmlinuz-2.4.2
  label=linux
  initrd=/boot/initrd-2.4.2.img
  read-only
  root=/dev/hda8
```

After:

```
boot=/dev/hda
map=/boot/map
prompt
default=argus
image=/boot/vmlinuz-2.4.17-argus1
  label=argus
  read-only
  root=/dev/hda8
image=/boot/vmlinuz-2.4.2
  label=linux
  initrd=/boot/initrd-2.4.2.img
  read-only
  root=/dev/hda8
```

Note: Your `/etc/lilo.conf` may not follow the same format as the above examples. The default image tag may be absent. If this is the case, the default image is the first image entry and the argus image entry should be placed as the first image entry.

Configuring `grub`

1. Open grub's configuration file (`/boot/grub/grub.conf` or `/boot/grub/menu.lst`) for editing.
2. Copy the currently used title entry, removing any initrd tags.
3. Edit the title tag to reflect the new kernel.

   `title PitBull LX for Linux (2.4.17-argus1)`

4. Change the kernel tag to reflect the new kernel.

   `kernel /vmlinuz-2.4.17-argus1`(options)

5. Save and close the configuration file.

Sample before and after configuration files are shown below (bold type indicates a change):

Before:

```
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Linux (2.4.2)
      root (hd0,0)
     kernel /vmlinuz-2.4.2 ro root=/dev/hda5
     initrd /initrd-2.4.2.img
```

After:

```
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title PitBull LX for Linux (2.4.17-argus1)
       root (hd0,0)
       kernel /vmlinuz-2.4.17-argus1 ro root=dev/hda5
title Linux (2.4.2)
      root (hd0,0)
      kernel /vmlinuz-2.4.2 ro root=/dev/hda5
      initrd /initrd-2.4.2.img
```

Note: In this example, we will be making PitBull the default kernel by adding to the default slot (0 in this case, as indicated by the `default=0` entry.)

Reboot

You must reboot the system for the changes to take effect.

Post-Installation

The product is now ready for configuration. The PitBull LX Administration Guide explains PitBull LX features in detail and provides exercises. Make sure you thoroughly understand the product before configuring your system for PitBull LX security.

Operating System Patch Procedure/Policy

In some cases, operating system patches require Argus modifications to properly operate with our security mechanisms. Please check the Support area of the Argus website (www.argus-systems.com) before installing any operating system patches on an Argus system. Compatibility lists, installation procedures, and properly modified versions of operating system patches are provided there.

WARNING: Installing operating system patches without first verifying that it is safe to do so on a system with Argus security mechanisms in place could cause system instability or even total operational failure.

Latest Updates

For the latest updates to documentation and patches for this product, check the Support section of our web site at www.argus-systems.com.

Technical Support

For technical support, contact Argus at: