

# Linux for computer forensic investigators: problems of booting trusted operating system

Author: Suhanov Maxim

ITDefence.Ru

## Introduction

This work is a part of series of papers titled «Linux for computer forensic investigators» and discusses problems appearing while booting several forensic Linux Live CD distributions based on Ubuntu (Debian).

## Boot process of Ubuntu-based distributions

The process of booting forensic Linux Live CD distributions based on Ubuntu consists of several steps:

1. The BIOS code runs the bootloader (e.g. GRUB);
2. The bootloader loads the Linux kernel and passes control to it. The kernel unpacks *initrd* image and executes */init* script;
3. */init* script runs several Casper scripts, that are used to search for the block device with a root file system image (e.g. SquashFS). During the search Casper scripts try to determine the file system type on a selected block device; if the file system type is supported by boot environment then Casper scripts mount the file system to «/cdrom» directory; then Casper scripts try to locate a root file system image on the mounted file system with optional UUID check for the media;
4. */init* script mounts the root file system image to «/root» directory and executes */root/sbin/init* program that will continue the boot process.

The same boot sequence is used in grml Live CD (based on Debian).

## Casper caveats

Casper scripts may mount file systems on evidentiary media (using only «-o ro» option) to find the right block device with root file system image. In some cases this will result in writes to the evidentiary media (the problem was discussed in previous paper).

Casper scripts will search for a root file system image by looking for files with specified mask (for example, «\*.squashfs») in a certain directory (for example, «/cdrom/casper»). After a file with «.squashfs» extension was found an optional UUID check may be launched (UUID check compares UUID values in file */cdrom/.disk/casper-uuid-generic* [located at the mounted CD file system] and in file */conf/uuid.conf* [located in the *initrd*]).

Then */init* script mounts discovered root file system image and executes *init* program (located at the mounted root file system) that will continue the boot process.

## The possibility of spoofing the operating system being loaded

Since there are no authenticity checks (except UUID check) for a root file system image, it is possible to spoof the operating system during the boot.

For example, Casper scripts may mount root file system from image located *on evidentiary media* (e.g. HDD). This root file system may have malicious */sbin/init* program that will wipe the evidence.

```

Welcome to

  G R M L
  G R M L
  G R M L

grml.org - Linux for sysadmins and texttool users.

* Running grml 2009.10 Release Codename Hello-Wien [2009-10-31]
* Finished early booting sequence. [ ok ]
* Searching for GRML file, this might take a few seconds...
* Setting device /dev/sda to read-only mode: done [ execute "blockdev --setrw /dev/sda " to unlock]
* Setting device /dev/sda1 to read-only mode: done [ execute "blockdev --setrw /dev/sda1" to unlock]
* Setting device /dev/sda2 to read-only mode: done [ execute "blockdev --setrw /dev/sda2" to unlock]
* Setting device /dev/sdb to read-only mode: done [ execute "blockdev --setrw /dev/sdb " to unlock]
* Setting device /dev/sdb1 to read-only mode: done [ execute "blockdev --setrw /dev/sdb1" to unlock]
  -> Mounted live system on /dev/sdb1
mount: mounting /dev/sda1 on /live/image failed: Invalid argument
/scripts/live-bottom/23networking: line 44: can't create /root/etc/network/interfaces: nonexistent directory
EVIL CODE EXECUTED! xD

Try another forensic Live CD...

```

*grml successfully executed malicious init program  
from a hard disk drive*

### **Forensic Linux Live CD distributions affected by this bug**

<u>Distribution</u>	<u>Web site</u>
Helix3 Pro 2009R2	<a href="http://www.e-fense.com/helix3pro.php">http://www.e-fense.com/helix3pro.php</a>
Helix3 2009R1	<a href="http://www.e-fense.com/helix3-download.php">http://www.e-fense.com/helix3-download.php</a>
CAINE 1.5	<a href="http://www.caine-live.net/">http://www.caine-live.net/</a>
DEFT Linux 5	<a href="http://www.deftlinux.net/">http://www.deftlinux.net/</a>
Raptor 20091026	<a href="http://www.raptorforensics.com/">http://www.raptorforensics.com/</a>
SMART Linux (Ubuntu) 2009-11-11	<a href="http://asrdata2.com/">http://asrdata2.com/</a>
grml 2009.10	<a href="http://grml.org/">http://grml.org/</a>
BackTrack 4 Pre	<a href="http://remote-exploit.org/">http://remote-exploit.org/</a>

### **Several ways to fix the issue**

There are several possible ways to fix the issue:

1. Do not use Casper scripts for booting;
2. Make UUID check mandatory and keep UUID in secret;
3. Enable hash values calculation and checking for discovered root file system images.

### **Conclusions**

I have found that all popular forensic Linux Live CD distributions based on Ubuntu (Debian) do not guarantee the authenticity of an operating system being loaded. Although the possibility of such attack is low, developers of forensic Linux distributions should take measures to fix the issue and enable operating system authentication.