# Implementing a System Call on Linux 2.6 for i386


## Amit Choudhary

`<amit2030 AT gmail DOT com>`



2006−10−27

**Revision History**

| | | |
|---|---|---|
| Revision 1.0 | 2006−10−27 | Revised by: ac |
| official release | | |



This HOWTO describes information about implementing system calls in the Linux operating system for i386 architecture with 2.6 kernels. General information about the used and modified files is available as well as description of the source and makefiles and test user space C program too.

# Table of Contents

1. Introduction........1
2. System call........2
3. List of files to be modified/created........3
4. Kernel files to be modified........4
5. syscall_table.S........5
6. unistd.h........6
7. syscalls.h........7
8. Makefile........8
9. New kernel files/directories to be created........9
10. mycall........10
11. mycall.c........11
12. Makefile........12
13. New user space files, to be created, to test our system call........13
14. testmycall.h (new user space header file to be created)........14
15. testmycall.c (new user space source file to be created)........15
16. _syscallN macro........16
17. Testing our new system call........17
18. Questions And Suggestions........18
19. Copyright........19
20. License........20

# 1. Introduction

This document explains how to implement a new system call on linux 2.6. A system call is used by application (user) programs to request service from the operating system.

# 2. System call

A system call is used by application (user) programs to request service from the operating system. The following statements illustrate why system calls are needed. An operating system can access a system's hardware directly, but a user program is not given direct access to the hardware. This is done so that the kernel can keep the system safe and secure from malicious user programs. But often, a user program requires some information from the hardware (e.g., from a web camera to show you the picture), but it cannot get the information directly. So, it requests the operating system to supply it the information. This request is made by using an appropriate system call.

A system call executes in the kernel mode. Every system call has a number associated with it. This number is passed to the kernel and that's how the kernel knows which system call was made. When a user program issues a system call, it is actually calling a library routine. The library routine issues a trap to the Linux operating system by executing INT 0x80 assembly instruction. It also passes the system call number to the kernel using the EAX register. The arguments of the system call are also passed to the kernel using other registers (EBX, ECX, etc.). The kernel executes the system call and returns the result to the user program using a register. If the system call needs to supply the user program with large amounts of data, it will use another mechanism (e.g., copy_to_user call).

# 3. List of files to be modified/created

Assume that your linux source base directory is /usr/src/linux.

Kernel files to be modified are listed below:

1. /usr/src/linux/arch/i386/kernel/syscall_table.S

2. /usr/src/linux/include/asm–i386/unistd.h

3. /usr/src/linux/include/linux/syscalls.h

4. /usr/src/linux/Makefile

New kernel files/directories to be created are listed below:

1. /usr/src/linux/mycall – Directory that will contain the source file, header file and the Makefile for our system call (You can also implement your system call in an existing file).

2. /usr/src/linux/mycall/mycall.c – Source file containing our system call code.

3. /usr/src/linux/mycall/Makefile – Makefile

New user space files, to be created, to test our system call are listed below:

1. testmycall.c â€“ Source file that will call our system call.

2. testmycall.h – Header file.

---

# 4. Kernel files to be modified

# 5. syscall_table.S

Full path of the file – /usr/src/linux/arch/i386/kernel/syscall_table.S

This file contains system call names.

1. Add a line to the end of this file (Let's assume that the name of our system call is mycall).
2. Add ".long sys_mycall" at the end of the list.

---

# 6. unistd.h

Full path of the file − /usr/src/linux/include/asm−i386/unistd.h

This file contains the system call number that is passed to the kernel through the register (EAX) when a system call is invoked.

1. Add "#define __NR_mycall <Last_System_Call_Num + 1>" at the end of the list.

If the last system call defined here is:

"#define __NR_vmsplice316", then add:

"#define __NR_mycall317" at the end of the list.

1. Increment the "NR_syscalls" by 1. So, if NR_syscalls is defined as:

"#define NR_syscalls 317", then change it to:

"#define NR_syscalls 318"

# 7. syscalls.h

Full path of the file – /usr/src/linux/include/linux/syscalls.h

This file contain the declarations for system calls.

1. Add the following line at the end of the file:

"asmlinkage long sys_mycall(int i);"

---

# 8. Makefile

Full path of the file – /usr/src/linux/Makefile

1. Add mycall/ to core−y (Search for regex: core−y.*+=). You will be creating this directory. This directory will contain the source file, header file and the Makefile for our system call.

# 9. New kernel files/directories to be created

# 10. mycall

Full path of the file – /usr/src/linux/mycall

1. Create a new directory in /usr/src/linux and name it "mycall".

---

# 11. mycall.c

Full path of the file – /usr/src/linux/mycall/mycall.c

1. Create a source file named "mycall.c" in dir "mycall". mycall.c will have the code for our system call. The definition of the system call in the source file would be asmlinkage long sys_mycall(...){...} . It should include the file linux/linkage.h So, the file "mycall.c" will look like:

```
/*−−−Start of mycall.c−−−−*/

#include<linux/linkage.h>

asmlinkage long sys_mycall(int i)

{

return i+10;

}

/*−−−End of mycall.c−−−−−−*/
```

What is asmlinkage?

Asmlinkage is used to look for the arguments on the kernel stack.

---

# 12. Makefile

Full path of the file – /usr/src/linux/mycall/Makefile

The Makefile in dir "mycall" will have only one line:

#####Makefile Start#####

obj−y := mycall.o

#####Makefile End#######

# 13. New user space files, to be created, to test our system call

# 14. testmycall.h (new user space header file to be created)

testmycall.h

1. Create a header file called testmycall.h. This header file should be included by any program calling our system call.
2. Add three lines to it

1. Line 1: This is needed because we need the definition of _syscall1.

#include<linux/unistd.h>

1. Line 2: This is needed because we need the number of our system call.

#define __NR_mycall 317

1. Line 3: This is needed for system calls with 1 argument. It is explained in detail below.

_syscall1(long, mycall, int, i)

So, our user header file looks like:

/*−−−Start of header file−−−−−−*/

#include<linux/unistd.h>

#define __NR_mycall 317

_syscall1(long, mycall, int, i)

/*−−−End of header file−−−−−−−−*/

# 15. testmycall.c (new user space source file to be created)

testmycall.c

1. Create a C file called testmycall.c in the same directory as testmycall.h. The C file will look like:

```
/*–––Start of C file––––––*/

#include<stdio.h>

#include "testmycall.h"

int main(void)

{

printf("%d\n", mycall(15));

}

/*–––End of C file––––––*/
```

# 16. _syscallN macro

1. _syscall0(int,mycall) indicates that:
2. The name of the system call is mycall.
3. It takes zero arguments.
4. It returns an int.

1. _syscall1(int,mycall,int,number) indicates that:
2. The name of the system call is mycall.
3. It takes one argument.
4. The argument is an int named number.
5. It returns an int.

When you expand _syscall1(long,mycall,int,i), you get the following code:

```
long mycall(int i)

{

return syscall(__NR_mycall, i);

}
```

But the definition of _syscallN macros are different in the kernel. You can look at /usr/src/linux/include/asm−i386/unistd.h for the definition.

# 17. Testing our new system call

1. Step 1: Recompile and install the new kernel so that our system call becomes available to the operating system.
2. Step 2: Compile and execute the user space C file (testmycall.c) that we created above.
3. RESULT: You should see the output as 25. This has been tested on kernel 2.6.17.13.

# 18. Questions And Suggestions

1. Please send a mail to Amit Choudhary (amit2030 AT gmail DOT com).

# 19. Copyright

# 20. License

GNU Free Documentation License

Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110–1301 USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world−wide, royalty−free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front−matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front–Cover Texts or Back–Cover Texts, in the notice that says that the Document is released under this License. A Front–Cover Text may be at most 5 words, and a Back–Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine–readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard–conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine−generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front−Cover Texts on the front cover, and Back−Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition.

Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine−readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer−network location from which the general network−using public has access to download using public−standard network protocols a complete Transparent copy of the Document, free of added material.

If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section

public access to a Transparent copy of the Document, and likewise

the network locations given in the Document for previous versions

it was based on. These may be placed in the "History" section.

You may omit a network location for a work that was published at

least four years before the Document itself, or if the original

publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications",

Preserve the Title of the section, and preserve in the section all

the substance and tone of each of the contributor acknowledgements

and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document,

unaltered in their text and in their titles. Section numbers

or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section

may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements"

or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front−matter sections or

appendices that qualify as Secondary Sections and contain no material

copied from the Document, you may at your option designate some or all

of these sections as invariant. To do this, add their titles to the

list of Invariant Sections in the Modified Version's license notice.

These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains

nothing but endorsements of your Modified Version by various parties−−for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front−Cover Text, and a passage of up to 25 words as a Back−Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front−Cover Text and one of Back−Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit.

When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

If you have Invariant Sections, Front−Cover Texts and Back−Cover Texts,

replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the

Front−Cover Texts being LIST, and with the Back−Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other

combination of the three, merge those two alternatives to suit the

situation.

If your document contains nontrivial examples of program code, we

recommend releasing these examples in parallel under your choice of

free software license, such as the GNU General Public License,

to permit their use in free software.