Baby steps to kernel hacking..

Sayli Karnik <karnisksayli1995@gmail.com>
The Linux kernel

- One of the biggest and fastest moving open source project
- 53600 files, >2M Loc
Maintainer Model

15600 coders!

Developer → Maintainer → Maintainer → Maintainer → Maintainer → Developer → Developer → Developer
Contributing to the kernel

• Step 1
  – Install Ubuntu/Debian
  – Setup tools:
    Editor (Eg. vim, gedit etc)
    Email client (Eg. Mutt)
    VCS (git)
Step 2

Linux kernel code repository

git clone -b staging-testing git://git.kernel.org/pub/scm/linux/kernel/git/gregkh/staging.git

Copy your current config

cp /boot/config-`uname -r`* .config

intern@ubuntu:~$ ls
COPYING  Documentation  Kconfig  Makefile  arch  certs  drivers  fs  init  kernel  mm  s
amples  security  tools  virt
CREDITS  Kbuild  MAINTAINERS  README  block  crypto  firmware  include  ipc  lib  net  s
cripts  sound  us
The Linux kernel

Step 3
Build/Install your kernel

```
make -jX

sudo make modules_install install
```
The Linux kernel

Step 4

- Make your branch
  - `git checkout -b first-patch`

- Update your kernel
  - `git fetch origin`
  - `git rebase origin/staging-testing`

- Make changes //TODO
- Re-Compile
• Step 5 - Get, set, go! ~> Commit, patch, email

```
git add <file>
git commit -s -v
git format-patch -o /tmp/ HEAD^  
```

0001-xyz.patch
**staging: media: davinci_vpfe: Use BIT macro instead of left shifting 1**

This patch replaces left shifts on 1 with the BIT(x) macro, as suggested by checkpatch.pl.
This was done using coccinelle script:

```c
@@
constant c;
@@
  (1 << c)
+ BIT(c)
```

Signed-off-by: sayli karnik <karniksayli1995@gmail.com>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

<table>
<thead>
<tr>
<th>Diffstat</th>
</tr>
</thead>
<tbody>
<tr>
<td>RWf---</td>
</tr>
</tbody>
</table>

1 files changed, 18 insertions, 18 deletions

```diff
diff --git a/drivers/staging/media/davinci_vpfe/davinci_vpfe_user.h b/drivers/staging/media/davinci_vpfe/davinci_vpfe_user.h
index 54f35c9..d3f34f9 100644
--- a/drivers/staging/media/davinci_vpfe/davinci_vpfe_user.h
+++ b/drivers/staging/media/davinci_vpfe/davinci_vpfe_user.h
@@ -544,41 +544,41 @@ struct vpfe_isif_raw_config {
     /**************************************************************************/
     /* IPIPE module configurations */
     /*#define VPFE_IPIFE_INPUT_CONFIG (1 << 0)
     +#define VPFE_IPIFE_INPUT_CONFIG BIT(0)
     /* LUT based Defect Pixel Correction */
     /*#define VPFE_IPIFE_LUTDPC (1 << 1)
     +#define VPFE_IPIFE_LUTDPC BIT(1)
     /* On the fly (OTF) Defect Pixel Correction */
```
• **Step 5..**

Shoot the email

```
mutt -H /tmp/0001--<whatever your filename is>
```

```
$ perl scripts/get_maintainer.pl --separator, --nokeywords --nogit --nogit-fallback --noroles
tats --nol -f drivers/staging/most/aim-sound/sound.c
Greg Kroah-Hartman <gregkh@linuxfoundation.org>
```
What can I change in the kernel?

- Starters
  - Code cleanups

```bash
intern@ubuntu:~/git/kernels/staging$ ls
COPYING  Documentation  Kconfig  Makefile  arch  certs  drivers  fs  init  kernel  mm  s
amples  security  tools  virt
CREDITS  Kbuild  MAINTAINERS  README  block  crypto  firmware  include  ipc  lib  net  s
cripts  sound  usr
```

```bash
perl scripts/checkpatch.pl -f drivers/staging/android/*/ | less
```

staging: rtl8192u: ieee80211: Remove typedef to the tx_pending_t structure

Using typedef for a structure type is not suggested in Linux kernel coding style guidelines. So remove typedef from structure tx_pending_t. The typedef name is not used anywhere. All variables of this type are declared using “struct tx_pending_t”. Also change the structure name to tx_pending since it is normally only typedefs that have names that end in _t.

Signed-off-by: sayli karnik <karniksayli1995@gmail.com>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

Diffstat
-rw-r--r-- drivers/staging/rtl8192u/ieee80211/ieee80211.h 6 6
1 files changed, 3 insertions, 3 deletions

diff --git a/drivers/staging/rtl8192u/ieee80211/ieee80211.h b/drivers/staging/rtl8192u/ieee80211/ieee80211.h
index 0971470..899c77e 100644
--- a/drivers/staging/rtl8192u/ieee80211/ieee80211.h
+++ b/drivers/staging/rtl8192u/ieee80211/ieee80211.h
@@ -1456,10 +1456,10 @@ enum ieee80211_state {

-typedef struct tx_pending_t{
+typedef struct tx_pending {
     int frag;
     struct ieee80211_txb *txb;
 } tx_pending_t;
+
     typedef struct _bandwidth_autoswitch {
         long threshold_20MHzto40MHz;
-      // -1833,7 +1833,7 @@ struct ieee80211_device {
-         RT_POWER_SAVE_CONTROL PowerSaveControl;
-       //}
-         /* used if IEEE_SOFTMAC_TX_QUEUE is set */
-     struct tx_pending_t tx_pend;
+     struct tx_pending tx_pend;
Staging: lustre: llite: rw26: Remove unused function definition

The patch removes unused function definition ll_get_user_pages().
The use of ll_get_user_pages() was replaced with iov_iter_get_pages_alloc() in commit 91f79c43d1b54d7154b118860d81b39bad07dfff.

Signed-off-by: sayli karnik <karniksayli1995@gmail.com>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

diffstat
-rw-r--r-- drivers/staging/lustre/lustre/llite/rw26.c 26

1 files changed, 0 insertions, 26 deletions

diff --git a/drivers/staging/lustre/lustre/llite/rw26.c b/drivers/staging/lustre/lustre/llite/rw26.c
index d89e795..420f296 100644
--- a/drivers/staging/lustre/lustre/llite/rw26.c
+++ b/drivers/staging/lustre/lustre/llite/rw26.c
@@ -156,32 +156,6 @@ static int ll_releasepage(struct page *vmpage, gfp_t gfp_mask)

#define MAX_DIRECTIO_SIZE (2 * 1024 * 1024 * 1024UL)

-static inline int ll_get_user_pages(int rw, unsigned long user_addr,
-                                       size_t size, struct page ***pages,
-                                       int *max_pages)
-{
-     int result = -ENOMEM;
-     
-     /* set an arbitrary limit to prevent arithmetic overflow */
-     if (size > MAX_DIRECTIO_SIZE) {
-         *pages = NULL;
-         return -EFBIG;
-     }
Some other coding style rules:

- Meaningful names: `cntusr()` → `count_users()`
- Not more than 80 columns
- Indentations/spaces/braces
- Avoid typedefs
- Standard commenting style
- Use existing macros
• Coccinelle can help!
(pattern matching and transformation tool)
Example:

```c
@depends on i@
type T; T[] E;
@@
- (sizeof(E)/sizeof(*E))
+ ARRAY_SIZE(E)
```
foo.cocci:
@ disable isnt_zero @
expression *E;
@@
E !=
- 0
+ NULL

make coccicheck MODE=patch
COCCI=scripts/coccinelle/api/err_cast.cocci

make coccicheck MODE=report M=drivers/net/

spatch --parse-cocci foo.cocci

spatch --sp-file foo.cocci foo.c
- Read kernel mailing archives
  \texttt{linux-kernel@vger.kernel.org}

Go through the git log to see commits

```bash
$ git log --pretty=oneline --abbrev-commit
fc17fe387718 Staging: tidspbridge: Fix split strings in drivers/staging/tidspbridge/core/tiomap3430.c
152cb4232c4f Staging: tidspbridge: Fix split strings in drivers/staging/tidspbridge/core/io_sm.c
4096ec993f10 staging: rts5139: Fix quoted string split across lines
```

**TODOs**

```bash
find drivers/staging -name TODO
```
• Sparse
• mixing of pointers to user and kernel address spaces, endianness bugs etc

Example:

```
$ sudo apt-get install sparse

$ make C=2 drivers/staging/wlan-ng/
```

Example:

```
typedef __u32 __bitwise __le32;
typedef __u32 __bitwise __be32;
```
• Smatch
• Uses sparse as C parser
• Use-after-free, buffer overflows, double/missing locks/unlocks etc.

~/progs/smatch/devel/smatch_scripts/kchecker drivers/whatever/

• https://lwn.net/Articles/691882/
Mark,
Lunch tomorrow sounds great! Let's keep it simple and get a pepperoni pizza.

> On Fri, Apr 26, 2013 at 9:25 AM, Mark wrote:
> Hey John, I had some questions I wanted to ask you:
> 1. Do you want to go out to lunch with me tomorrow?
> 2. What's your favorite type of pizza?
> 3. You're paying this time, right?

Mark,
See my answers below...
> On Fri, Apr 26, 2013 at 9:25 AM, Mark wrote:
> Hey John, I had some questions I wanted to ask you:
> 1. Do you want to go out to lunch with me tomorrow?
Lunch tomorrow sounds great!
> 2. What's your favorite type of pizza?
Let's keep it simple and get a pepperoni pizza.
> 3. You're paying this time, right?
You bet! You paid last time so it's my turn.
Subject: [PATCH v2 1/2] USB: at91: fix the number of endpoint parameter

In sama5d3 SoC, there are 16 endpoints, which is different with earlier SoCs (only have 7 endpoints). The USBA_NR_ENDPOINTS micro is not suitable for sama5d3. So, get the endpoints number through the udc->num_ep, which get from platform_data for non-dt kernel, or parse from dt node.

Signed-off-by: Bo Shen <voice.shen@atmel.com>
---
Changes in v2:
- Make the commit message more clearer.

drivers/usb/gadget/atmel_usba_udc.c | 2 ++
1 file changed, 1 insertion(+), 1 deletion(-)
diff --git a/drivers/usb/gadget/atmel_usba_udc.c b/drivers/usb/gadget/atmel_usba_udc.c
Resources

https://kernelnewbies.org
https://lwn.net

LKML mailing list
May the source be with you :)  

For further questions reach out to me at -  
karniksayli1995@gmail.com  
http://karniksayli.wordpress.com/