# Using Coccinelle

Peter Senna Tschudin (Inria/LIP6-Regal)

October 25, 2013

peter.senna@gmail.com (C0850387)

# Coccinelle

- Static analysis to find patterns in C code.
- Automatic transformation.
- User scriptable, based on patch notation (semantic patches).

http://coccinelle.lip6.fr/

http://coccinellery.org/

# Example: devm function usage

Devm functions:

- Provide allocation of managed memory.
- Allocate using a function whose name (typically) begins with `devm`
  - `kzalloc` $\Longrightarrow$ `devm_kzalloc`
- Free performed implicitly on error or resource remove.
  - `kfree` $\Longrightarrow$ nothing

# Example from Linux-next

## drivers/video/vt8500lcdfb.c

```
  fbi = devm_kzalloc(&pdev->dev, sizeof(struct vt8500lcd_info)
      + sizeof(u32) * 16, GFP_KERNEL);
  if (!fbi) {
    dev_err(&pdev->dev, "Failed to initialize framebuffer device");
    ret = -ENOMEM;
    goto failed;
  }
  ...
  res = platform_get_resource(pdev, IORESOURCE_MEM, 0);
  if (res == NULL) {
    dev_err(&pdev->dev, "no I/O memory resource defined");
    ret = -ENODEV;
    goto failed_fbi;
  }
  ...
failed_fbi:
  kfree(fbi);
failed:
  return ret;
```

# How to find these problems?

- Grep for `devm_kzalloc` gives too many things.
- Grep for `kfree` gives too many things.
- The relevant lines are far apart.

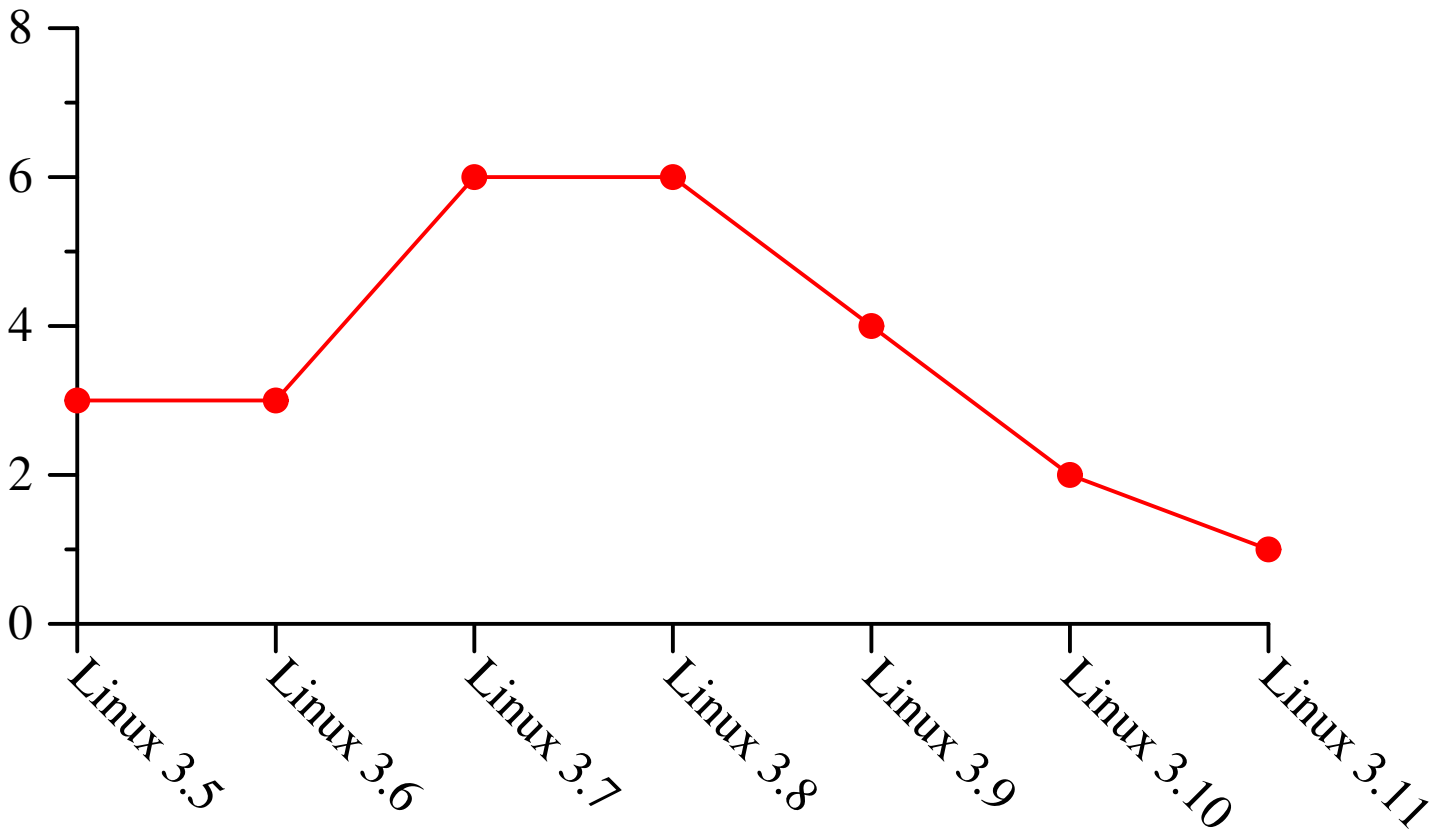
# Using Coccinelle

```
@@
expression x;
@@

* x = devm_kzalloc(...)
  ...
* kfree(x)
```

# Making the rule more robust

```
@@
expression x,e;
@@

* x = devm_kzalloc(...)
  ... when != x = e
* kfree(x)
```

# Results




No occurrences between 2.6.32 and 3.4, when `devm_kzalloc` was less used.

# What should we do next?

## Mailing list

- cocci@systeme.lip6.fr
- We are responsive!

## Examples to inspire users

- http://coccinellery.org/
- More than 300 semantic patches with simple descriptions

What should we do next?

`http://coccinelle.lip6.fr/`