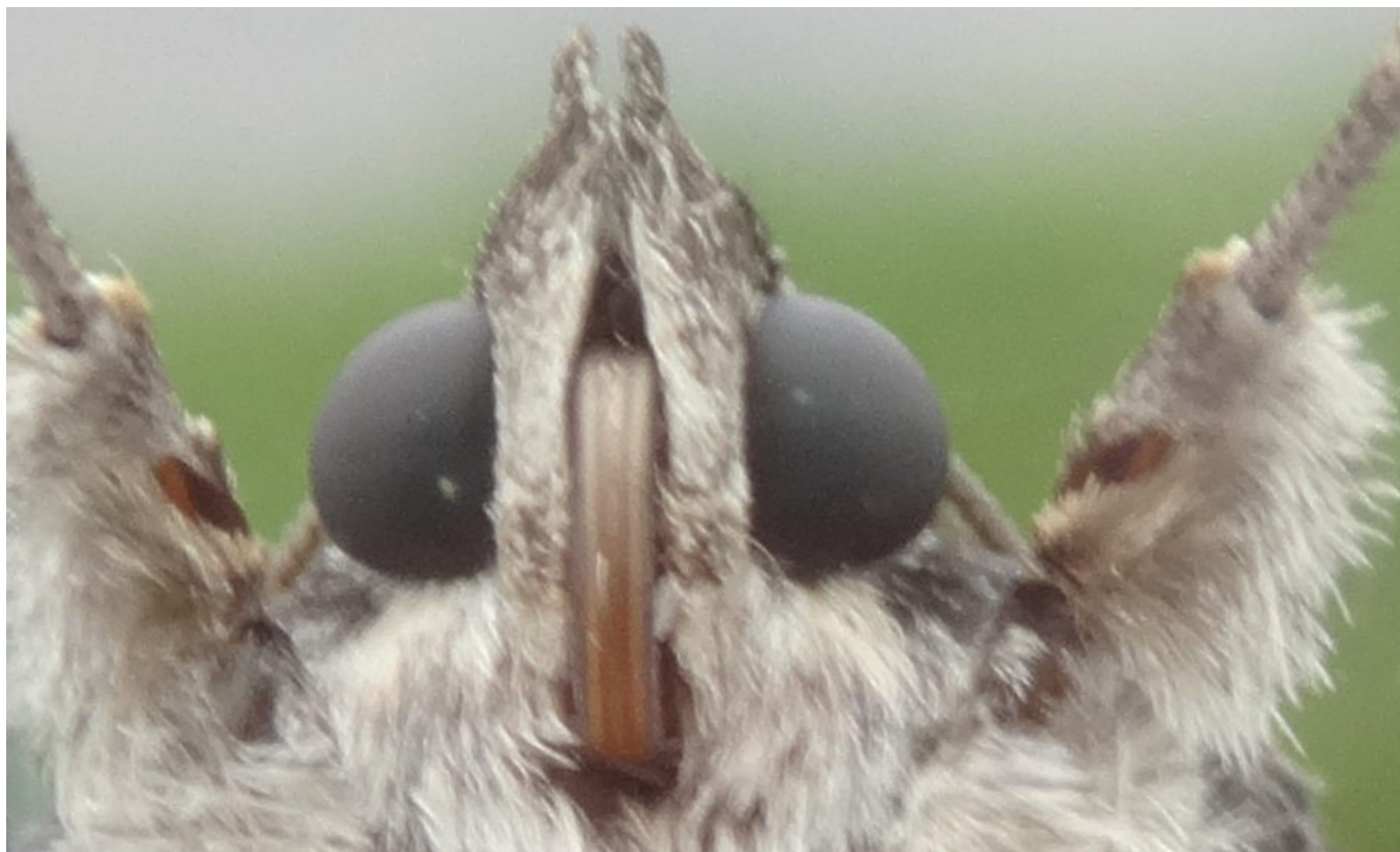


Fun bugs



Fun bugs [selection]

- ◆ **No security bugs**

Most of those are just hilariously stupid anyway!

- ◆ **Fun or interesting symptoms**

- ◆ **No direct deaths....**

- ◆ **Needed to find a reference**

Brother printers won't print OpenOffice docs on Tuesdays

<https://bugs.launchpad.net/ubuntu/+source/cupsys/+bug/255161>

- **People reported broken printing...that then started working...and then stopped**
- **Took ~8 months for someone to notice it only happened on Tuesdays - and the cause: 'file'/'magic' data misidentifying Postscript as a Erlang file**
- **OpenOffice produces PostScript output**
- **Printer driver detects file format**
- **Detection uses 'file'**

Brother printers won't print OpenOffice docs on Tuesdays [2]

%%CreationDate: (Tue Mar 3 19:47:42 2009)

- **'file' relies on a 'magic' description**
- **Mistake meant it recognised files with 'Tue' as an 'Erlang JAM file'**

- **Fun:**

Manual testing would depend which day of the week you tried it on

Problem is not in the printer driver or OpenOffice

Wake up to blink hidden cursor

<http://mirror.linux.org.au/pub/linux.conf.au/2007/video/talks/38.pdf>

- **Woke up ~5 times/second to blink console cursor**

→ Even when in X and it's invisible!

- **Power saving bugs can be tricky**

Not always obvious why/who woke up

```
Fedora 30 (MATE-Compiz)
Kernel 5.0.10-300.fc30.x86_64 on an x86_64 (tty2)

localhost login: _
```

[That slide set contains lots of other fun little bugs]

- **Fun: I like a bug you by definition can't see**

Integer overflows: Timers and crashes

Linux 208.5 days: <https://www.suse.com/support/kb/doc/?id=7009834>

Boeing 787 , 248 days: <https://www.federalregister.gov/documents/2015/05/01/2015-10066/airworthiness-directives-the-boeing-company-airplanes>

- ♦ **Integer counters have limited sizes**

e.g. $2^{31} \approx 2B = 248$ days at 100Hz

~ 68years at 1Hz - Unix Epoch in 2038

- ♦ **Overflows that fail quickly get spotted in test**
- ♦ **Overflows that take too long give years of warning - if spotted!**
- ♦ **The ones in the middle.....**
- ♦ **Fun: Redundant backups all fail at once!**

Image compression vs scanners

Youtube talk: <https://www.youtube.com/watch?v=c0O6UXrOZJo>

Blog: https://media.ccc.de/v/froscon2015-1524-lies_damned_lies_and_scans

• Xerox scanners over compressed substituting digits:

(c) David Kriese
cca
















	Original	WC 7535	WC 7556 (A)	WC 7556 (B)	WC 7556 (C)
Place 1					
Place 2					
Place 3					

Image compression vs scanners [2]

- ♦ **JPEG compresses by maths on individual blocks**
 - Stuff can look fuzzy, but rarely confusing
- ♦ **JBIG2 looks for blocks to copy**
 - i.e. only store one copy of a block – and hopefully fix up slight differences
 - Potential differences are confusing, convincing and unobvious
 - Now banned by German and Swiss regulators for archival use
 - Billions of scans already out there.
 - Thousands of scanners probably unpatched.

Leapseconds

Linux crashes: <https://lkml.org/lkml/2012/7/17/392>

Summary of leap second handling: <https://access.redhat.com/articles/15145>

IETF: <https://www.ietf.org/timezones/data/leap-seconds.list>

- **Atomic clocks more accurate than the earth**

- Needs an occasional fudge second
- Not regular, announced by committee, either direction, communicated [Politics failed to kill it off]

- **Repeated, 61 seconds, or smeared**

- Sometimers, not others!

- **Typically at end of Dec or Jun**

- **Table lists when it happened**

```
$ date; TZ=right/Europe/London date
Sun 12 May 20:09:58 BST 2019
Sun 12 May 20:09:31 BST 2019
```

Integer underflows: civilization vs Gandhi

<https://www.geek.com/games/why-gandhi-is-always-a-warmongering-jerk-in-civilization-1608515/>

- ◆ **Unsigned 8 bit integers**

0-1=255

- ◆ **Civilization used a 'aggressiveness' score**

Gandhi was very low (0 or 1)

- ◆ **-2 aggression level for a civilisation on adoption of democracy**

- ◆ **Aggression wraps**

Becomes a war monger!

Fun with `rm -rf` in scripts

Steam: <https://github.com/ValveSoftware/steam-for-linux/issues/3671>

Bumblebee: <https://github.com/MrMEEE/bumblebee-Old-and-abandoned/issues/123>

- ◆ **Not checking shell variables**

```
rm -rf "$STEAMROOT/"*
```

If `$STEAMROOT` is empty that's `rm -rf /*`

- ◆ **Errant spaces**

```
rm -rf /usr /lib/nvidia-current/xorg/xorg
```

Note the space after `'/usr'`

AI - adversarial attacks

<https://spectrum.ieee.org/cars-that-think/transportation/sensors/slight-street-sign-modifications-can-fool-machine-learning-algorithms>

<https://arxiv.org/abs/1707.08945>

- **Modern Neural networks/
deep learning/AI used all over**

e.g. sign recognition,
photo recognition, etc

- **No actual understanding**

Just a set of pixels, not 'stop' on an
octagonal red sign

- **Can be sensitive to certain
pixels**

- **Lots of funny examples - and potentially serious
ones**



Cascading failures

US 2003 blackout: https://en.wikipedia.org/wiki/Northeast_blackout_of_2003

Amazon AWS DB: <https://aws.amazon.com/message/5467D2/>

♦ **When a few small failures cause massive outages**

e.g. one or two high-capacity power lines vs trees

Major US power outage

Massive power swings, generators tripping etc

Included an alarm system failure for ~30mins so operators didn't know of some failures [caused by a race condition]

e.g. a momentary network blip

Amazon DynamoDB - network blip caused servers to check 'membership'

- That was a bit too slow - and a lot checking at once slowed it down
- ... and that caused other servers to fail and retry, causing it to slow.

Cascading failures [2]

- ◆ **Simple interacting rules + lots of parts**
 - Rules each look OK
 - but what happens when you take thousands of them
 - Difficult to know how small changes interact

“Emergent behaviour”

Mars Climate Orbiter: Metric vs US units

https://en.wikipedia.org/wiki/Mars_Climate_Orbiter

- **Results in lbf.s (pound-force seconds?!)**
- **Expected in N.s (Newton seconds)**
- **Ended up ~50 km too low**

Heisenbugs

- ◆ **More a general class of bugs**

Things that go away or change when you try and debug them

- * Timing (race conditions)
- * Address layouts (e.g. paths, environment variables)