Debian Long Term Support
The story of an unusual team

By Raphaël Hertzog <hertzog@debian.org>

Lyon Mini-DebConf / 2015-04-12

Plan of the talk

- Presentation of the LTS project/team
- Statistics about the team
- Current and future challenges
- Workflow of the team: how to contribute
- Questions
  - Feel free to ask questions at any time

Presentation of the LTS project

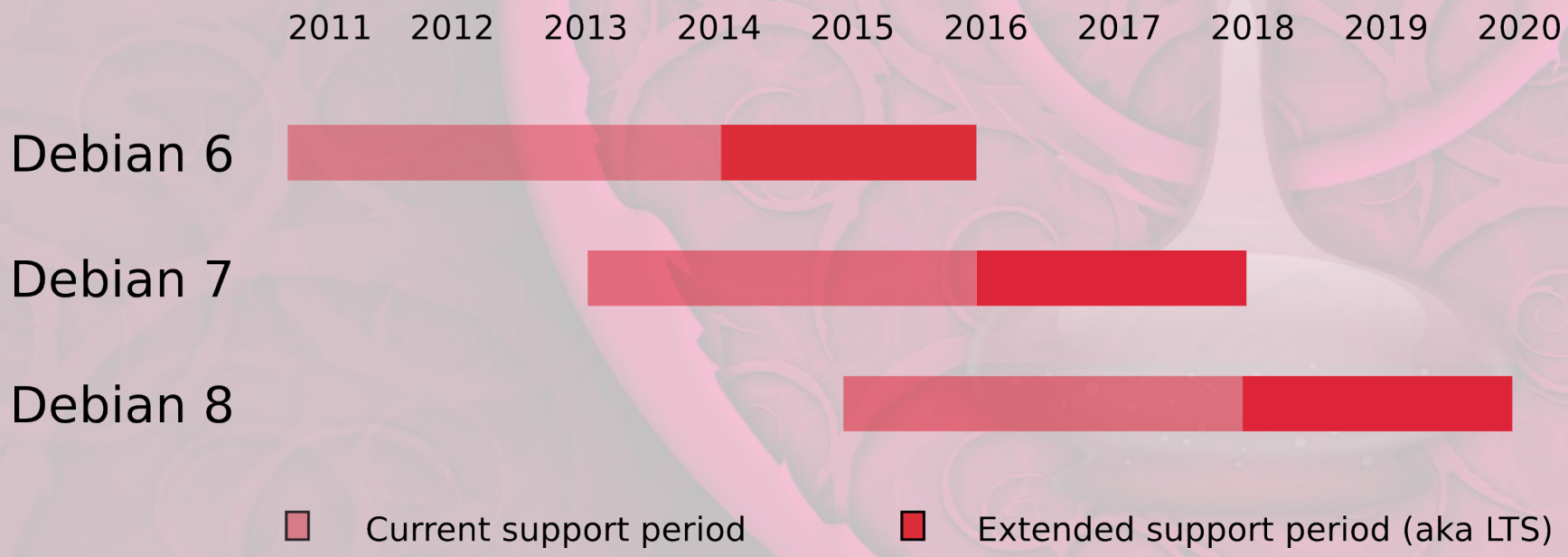
What is LTS about?

What were the challenges?

Choices made: at the technical level, at the organizational level

What is LTS about ?

- Providing 5 years of security support
- Thus allowing users to skip a release



Initial challenges

- Keeping a distribution secure for 5 years is hard work that is not very rewarding
- The security team
  - has limited resources
  - aims to support all Debian packages on all release architectures

Technical choices: restrict the perimeter

- Restrict architecture support to amd64 and i386
- Exclude some “problematic” packages from security support (~40 packages):
  - **asterisk**, axis2c, **bugzilla**, **chromium-browser**, couchdb, **drupal6**, ffmpeg, flashplugin-nonfree, fusionforge, gksu-polkit, gridengine, horde3, iceape, icedove, **iceweasel**, kolab-cyrus-imapd, libplrpc-perl, libv8, **libvirt**, mahara, mantis, **mediawiki**, moodle, movabletype-opensource, openswan, **qemu**, **qemu-kvm**, **rails**, serendipity, smarty, smarty3, spip, textpattern, turba2, typo3-src, vlc, **xen**, xen-qemu-dm-4.0, zabbix
  - http://anonscm.debian.org/cgit/collab-maint/debian-security-support.git/plain/security-support-ended.deb6

Organizational choice #1: creation of a new team

- Security team ≠ Debian LTS team
  - But members of the security team helped to bootstrap the LTS team
- Different policies
- Different infrastructure
  - Mailing list : debian-lts@lists.debian.org https://lists.debian.org/debian-lts/
  - IRC channel: #debian-lts on irc.debian.org (OFTC)

Organizational choice #2: seeking help of companies

- Try to pool the work of companies which were doing in-house long term security support already
  - Press release to invite companies to join
- Let other organizations fund the project so that Debian contributors can be paid to do the work
  - https://wiki.debian.org/LTS/Funding lists all ways to help with money
  - In practice, most of the (wanting to be) paid contributors joined forces behind a single offer managed by Freexian SARL : http://www.freexian.com/services/debian-lts.html

Freexian's intermediary role

Sponsors

Gold level

Silver level

Bla Bla Car

domainnameshop

evolix

gandi.net

Trollweb

Université Lille 3

Bronze level

bitfolk

DAEVEL

FOSSter

freeside

GREE

Greenbone

Intevation GmbH

linuxhotel

MEGASPACE

MyTux

NUMLOG

Nantes Métropole

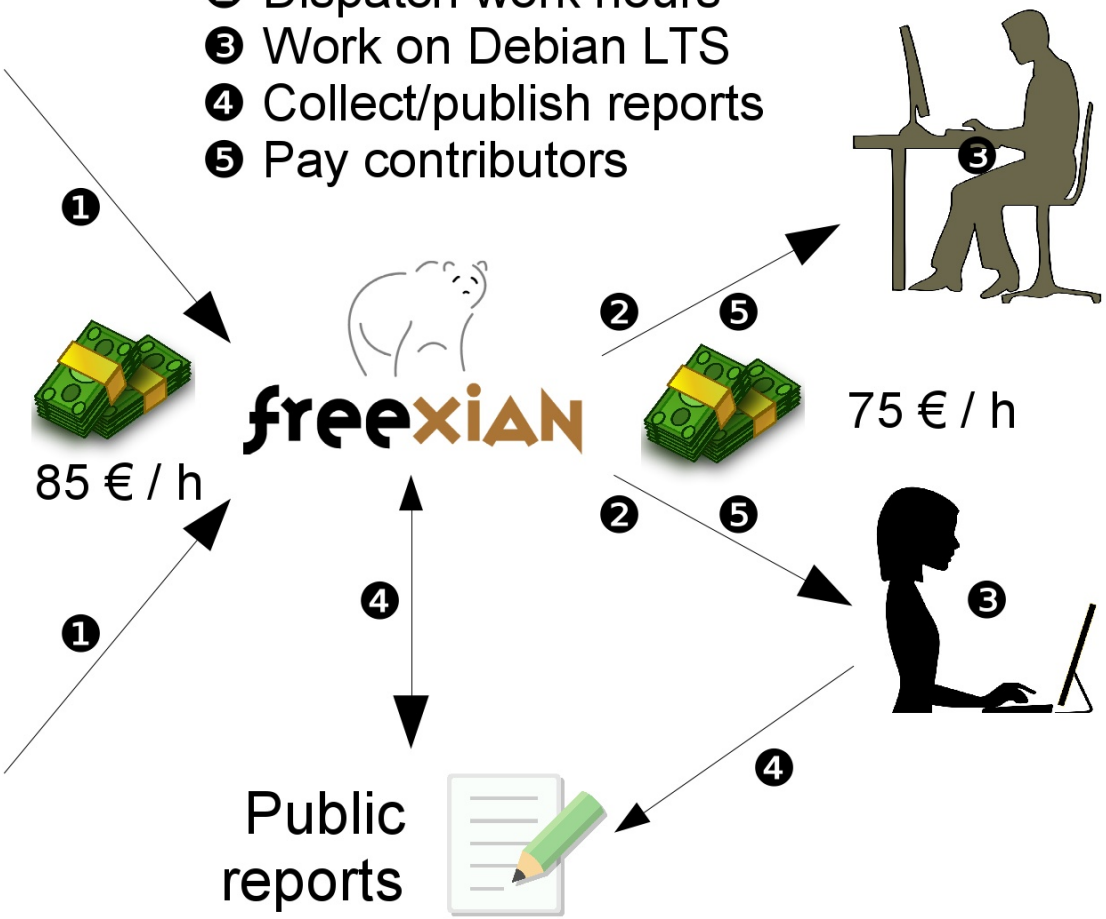
OFFENSIVE security

SEZNAM.cz

wingo

Contributors

1. Collect money
2. Dispatch work hours
3. Work on Debian LTS
4. Collect/publish reports
5. Pay contributors



Statistics about the team

Who uploaded packages?

How did it evolve since the beginning?

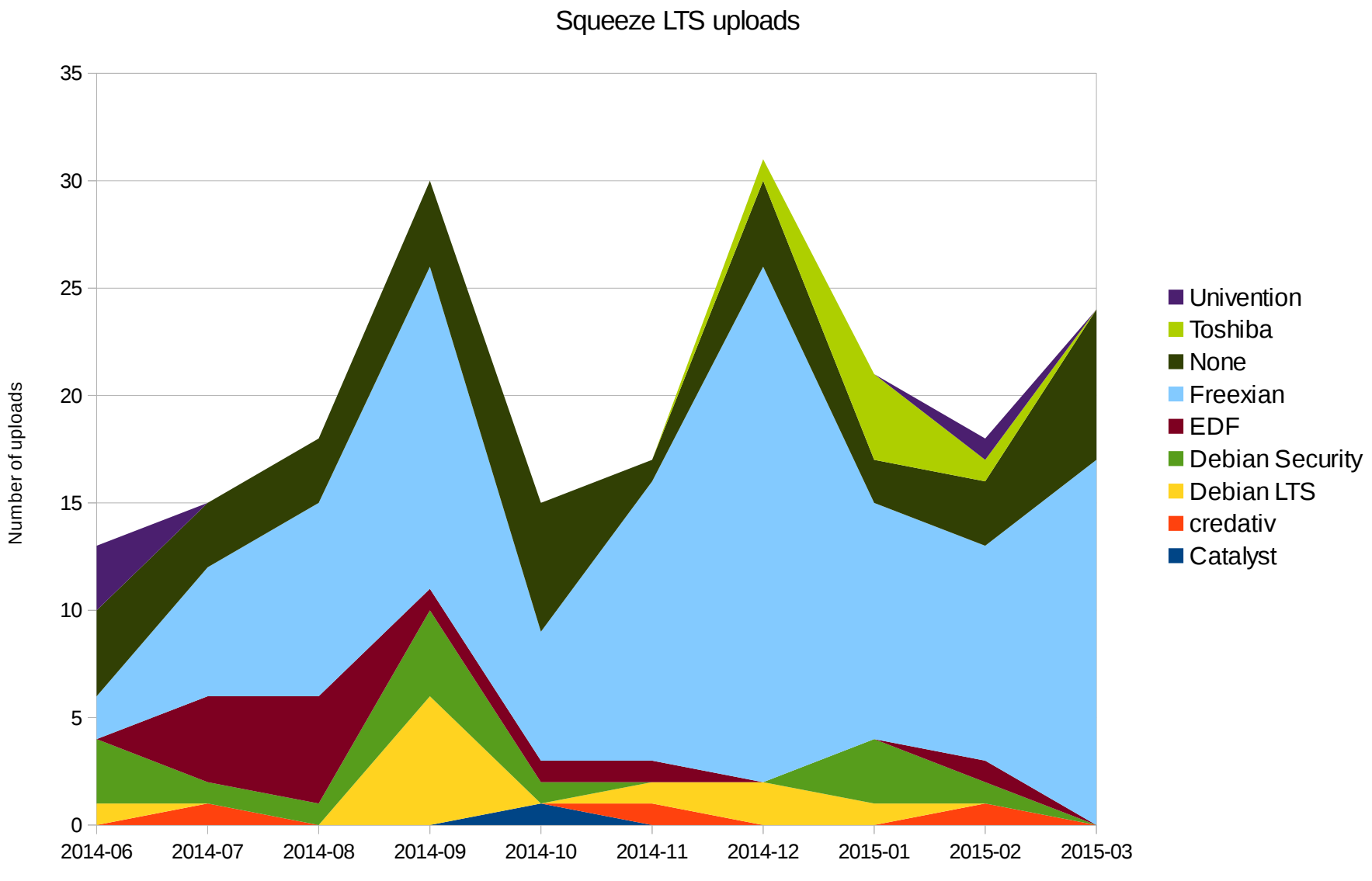
How is the funding evolving?

Data between 2014-06-01 and 2015-03-31

Stats: 202 squeeze-lts uploads

- By affiliation:
  - Freexian: 113
  - None (maintainers): 37
  - Security team: 14
  - EDF: 13
  - Individuals: 11
  - Toshiba: 6
  - Univention: 4
  - credativ: 3
  - Catalyst: 1
- By contributor:
  - Thorsten Alteholz: 66
  - Holger Levsen: 27
  - Raphaël Hertzog: 14
  - Raphaël Geissert: 13
  - Thijs Kinkhorst: 8
  - Kurt Roeck: 7
  - Christoph Biedl: 7
  - Nguyen Cong: 6
  - Ben Hutchings: 6
  - Michael Vogt: 5
  - Moritz Mühlenhoff: 4
  - Matt Palmer: 4

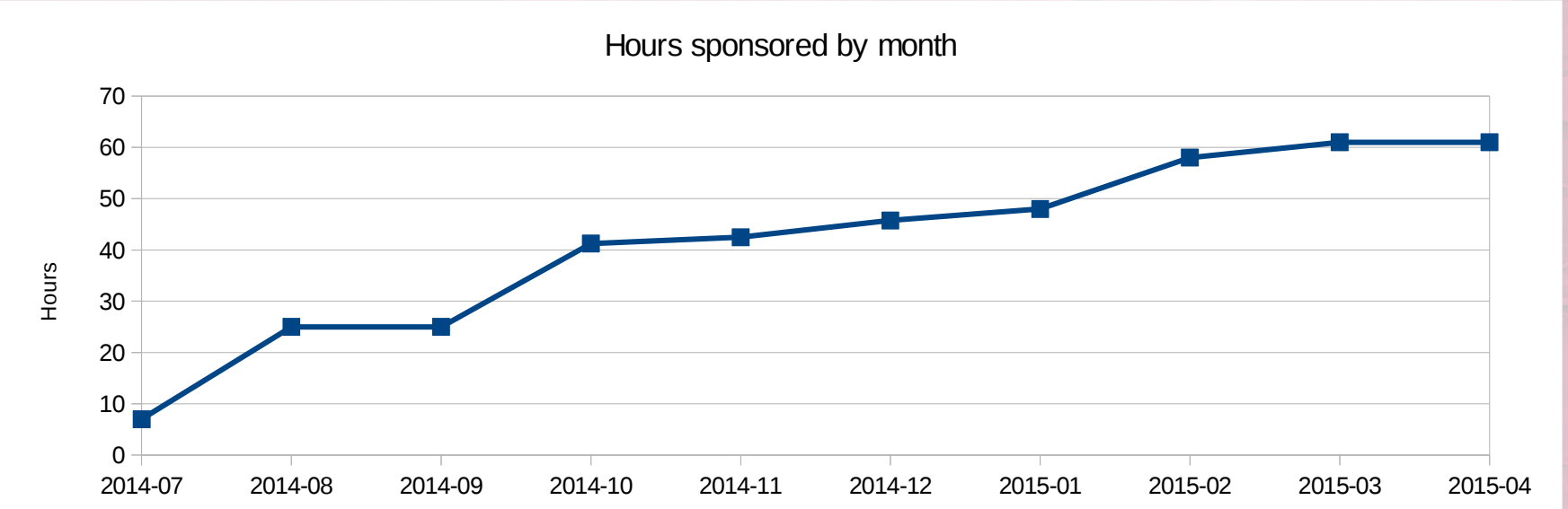
squeeze-lts uploads over time



Statistics about sponsored hours managed by Freexian

- Sponsors: 29
  - Gold (>= 8 h/month): 1
  - Silver (>= 4 h/month): 7
  - Bronze (>= 1h/month): 17
  - Iron (< 1 h/month): 4
- Average: 2.1 h/month/sponsor

- Hours sponsored
  - 61 h/month currently dispatched to 5 contributors
  - 444h since the start (230h already paid to be dispatched over the next year)



Current and future challenges

Keep supporting the current set of packages

Supporting more packages for Wheezy LTS

Ensure a smoother Wheezy LTS

→ this will be discussed in
a DebConf 15 Talk and BoF

Keep supporting the current set of packages until 2016

- How to handle MySQL?
  - Oracle does not provide details about CVE
    - no patches to backport
    - no way to ensure the CVE affect MySQL 5.1
  - MySQL 5.1 is no longer supported by Oracle
    - no new 5.1.x versions to import
  - Upgrading to MySQL 5.5 involves a library transition
    - not realistic with the current funding level
- Similar problems with other packages without upstream support
  - glassfish, wireshark, …

Supporting more packages for Wheezy LTS

- Many important packages are missing security support in Squeeze LTS
  - Not possible to run a Xen/KVM host (only guest)
  - No web application based on Ruby on Rails
  - No web browser (iceweasel/chromium)
- We need more resources to be able to commit to 5 years of support on such high profile packages
  - How to get help from more companies?

Ensure a smoother Wheezy LTS

- Problems/limitations of Squeeze LTS:
  - Users must add a new repository
  - No intermediary repository
    - To collect builds from all architectures
    - To ensure a minimal review before acceptance
  - Usage of normal mirror instead of security.debian.org
    - 6h propagation delay
    - Updates not identified as security updates by some tools (update-notifier, unattended-upgrades, monitoring checks, etc.)

Workflow of the team

Triage of security issues

Preparation of security update

Test of security update

Upload and announce of update

Triage of security issues

- Done in the security tracker (common to Debian Security and Debian LTS)
  https://security-tracker.debian.org/
  http://security-team.debian.org/security_tracker.html

1. New issues added to data/CVE/list
2. Issues dispatched on source packages
3. Issues reviewed for each release
4. Classification according to analysis

Ways to classify security issues

- Depending on analysis:
  - Package added to data/dla-needed.txt so that someone will take care of preparing the update (currently <unfixed>)
  - Issue does not apply (<not-affected>)
  - Issue ignored because package is not supported (<end-of-life>)
  - Issue not important enough (<no-dsa>)
  - Issue already fixed in a former version
- Keep the maintainers in the loop, they can always fix issues (even the non-important ones)

Extract of data/CVE/list

```
CVE-2015-2317 (The utils.http.is_safe_url function in Django…)
        {DSA-3204-1}
        - python-django 1.7.7-1 (bug #780873)
        [squeeze] - python-django <no-dsa> (Minor issue, can wait
next security upload)
        NOTE: https://github.com/django/django/commit/… (1.4.x)

CVE-2015-2189 (Off-by-one error in the pcapng_read…)
        {DSA-3210-1}
        - wireshark 1.12.1+g01b65bf-4 (bug #780372)
        [squeeze] - wireshark <not-affected> (Vulnerable code not
present)
        NOTE: https://bugs.wireshark.org/bugzilla/…

CVE-2014-9701 [XSS issue in MantisBT permalink_page.php]
        - mantis <removed> (bug #780875)
        [wheezy] - mantis <no-dsa> (Minor issue)
        [squeeze] - mantis <end-of-life> (Unsupported in squeeze-
lts)
        NOTE: Fixed by https://github.com/mantisbt/… (1.2.x)
```

Preparation of the security update

- Find a patch
- Backport it if required
- Prepare an upload with a “+deb6uX” suffix, applying the patch as appropriate
  - Document fixed CVE in the changelog and in patch headers

Test the update and upload

- Build and test the result to ensure that
  - the package still works
  - the fix works as expected
  - there's no obvious regression
- If unsure of your update, get in touch:
  - Ask others to test
  - Seek reviews of your debdiff
- If everything is ok, upload to squeeze-lts.

Announce the security update

- Prepare a “DLA” (Debian LTS Advisory)

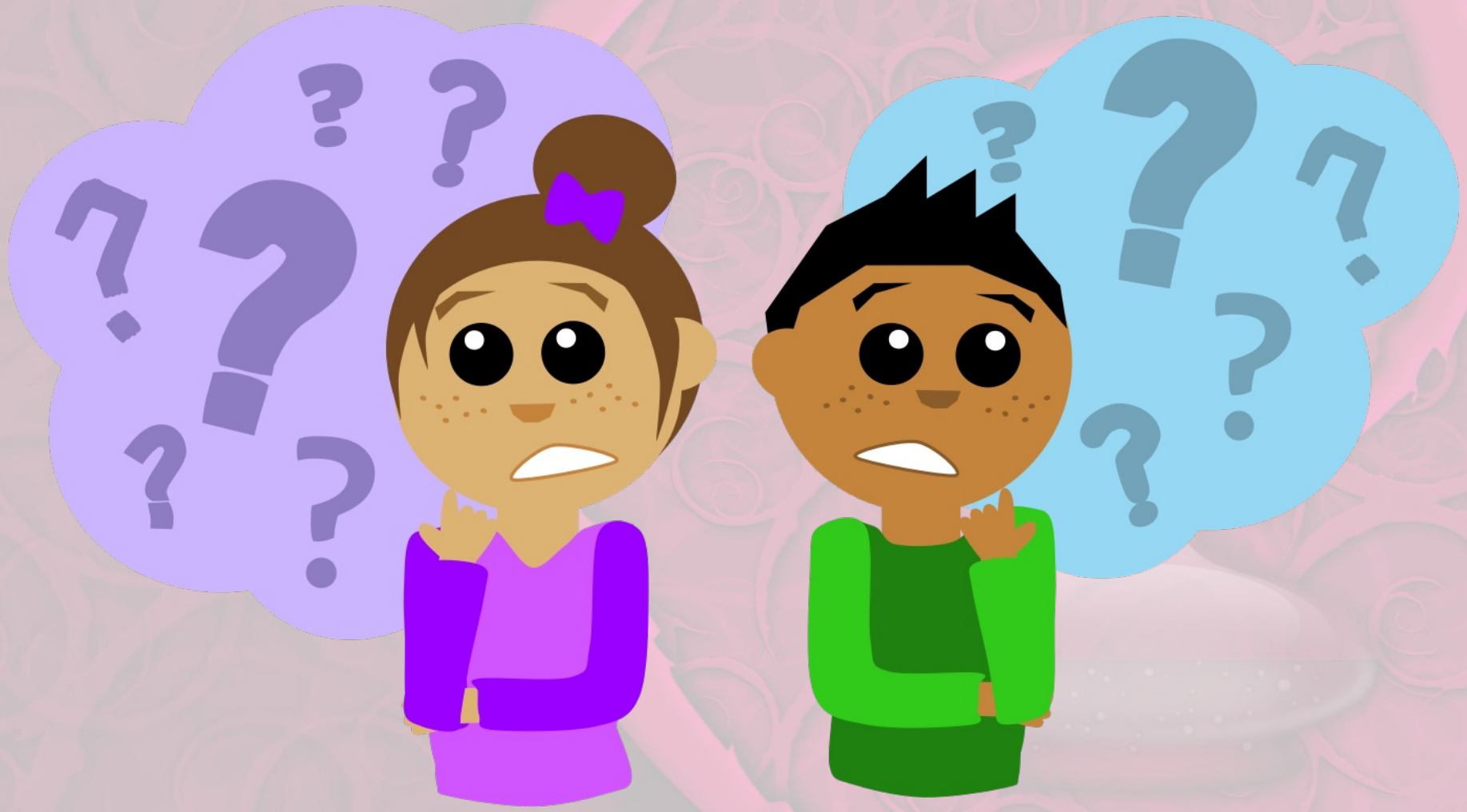
```
$ ./bin/gen-DLA --save libgd2 CVE-2014-2497 CVE-2014-9709
Enter squeeze's version [unset]: 2.0.36~rc1~dfsg-5+deb6u1
DLA text written to ./DLA-190-1
$ svn commit
```

- Send it to debian-lts-announce@lists.debian.org

```
$ mutt -H DLA-190-1
```

- This process updates `data/DLA/list` which is used by the security tracker to know the CVE fixed by the update

Questions ?



Credits & License

- Content by Raphaël Hertzog
  http://raphaelhertzog.com
  License: GPL-2+
- Cliparts from https://openclipart.org
  License: Public domain
- OpenOffice.org template by Raphaël Hertzog
  http://raphaelhertzog.com/go/ooo-template
  License: GPL-2+
- Background image by Alexis Younes “ayo”
  http://www.73lab.com
  License: GPL-2+