Reproducible Builds

Mattia Rizzolo
mattia@reproducible-builds.org

Ubuntu Conference
Riga, Latvia
4th November 2023

Debian Developer since 2015

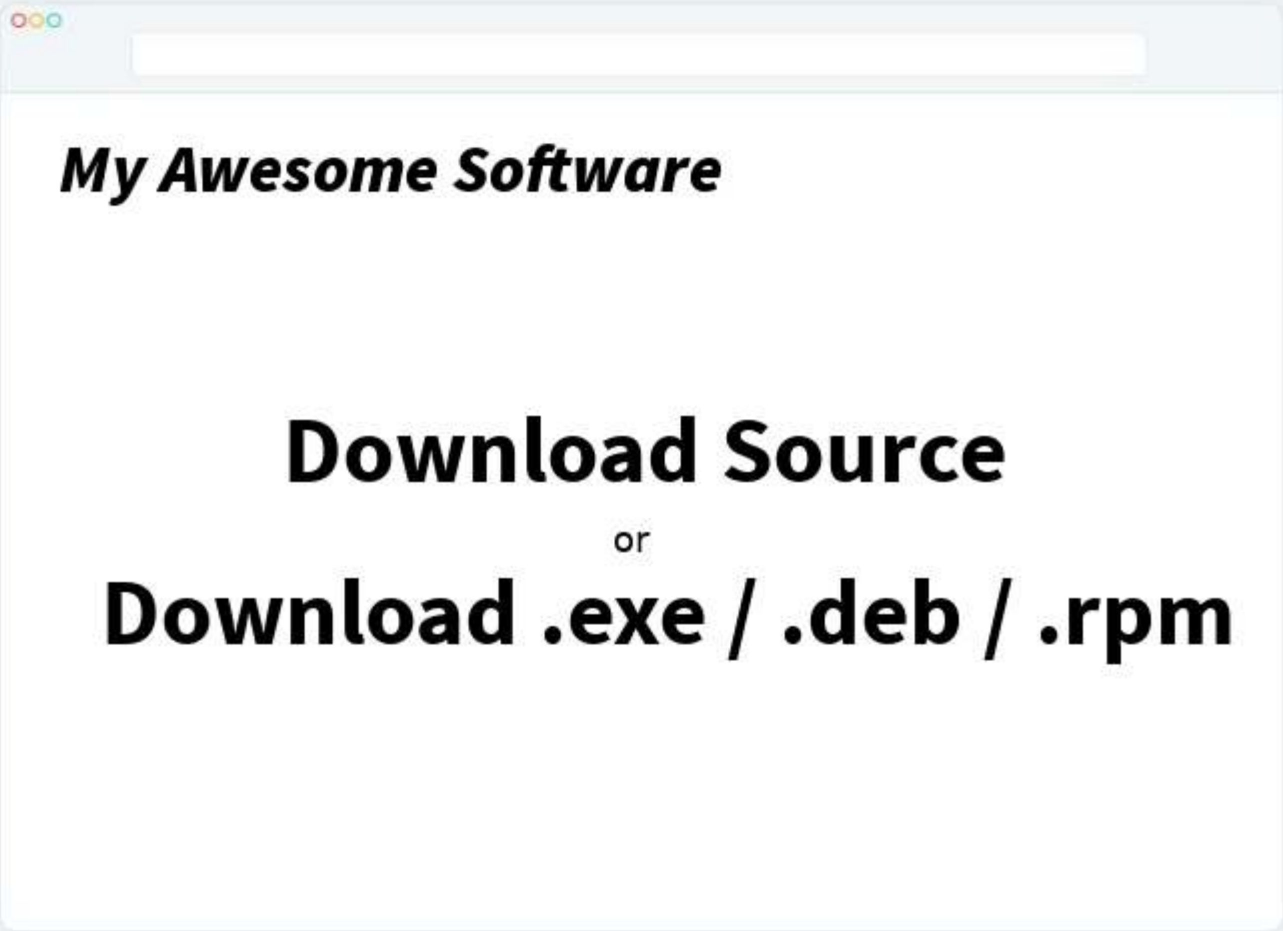
Ubuntu Member since 2013

Ubuntu Developer since 2016

Free software developer for ~10 years

Three developers…

Alice

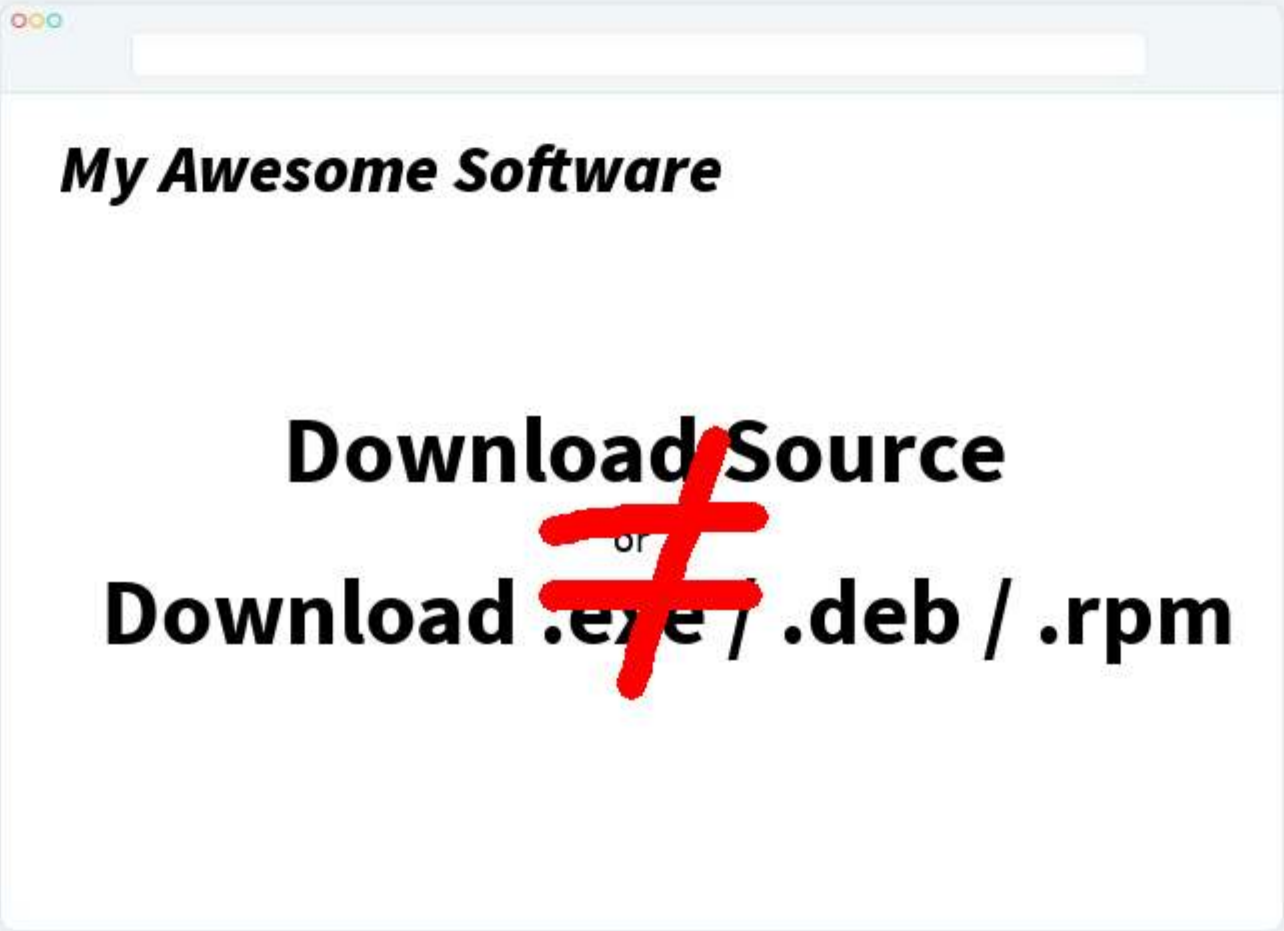


My Awesome Software

Download Source

or

Download .exe / .deb / .rpm



My Awesome Software

Download Source

≠

or

Download .exe / .deb / .rpm

Bob

← Caro

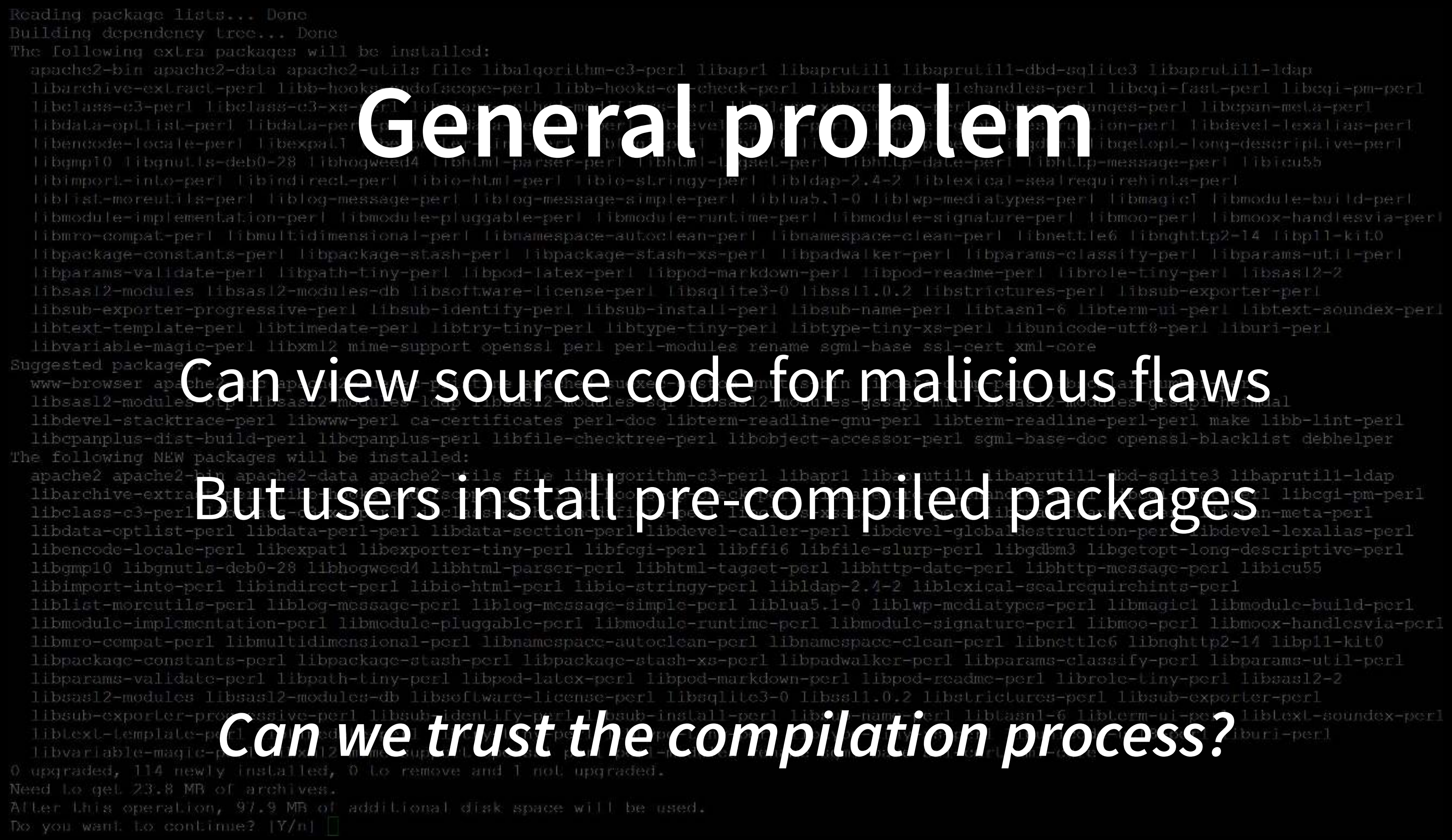
Eve →

General problem

Can view source code for malicious flaws

But users install pre-compiled packages

Can we trust the compilation process?



```
Reading package lists... Done
Building dependency tree... Done
The following extra packages will be installed:
  apache2-bin apache2-data apache2-utils file libalgorithm-c3-perl libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
  libarchive-extract-perl libb-hooks-[illegible]dofscope-perl libb-hooks-o[illegible]-check-perl libbar[illegible]ord-[illegible]lehandles-perl libcgi-fast-perl libcgi-pm-perl
  libclass-c3-perl libclass-c3-xs-[illegible]anges-perl libcpan-meta-perl
  libdata-optlist-perl libdata-per[illegible]ion-perl libdevel-lexalias-perl
  libencode-locale-perl libexpat1 [illegible] libgetopt-long-descriptive-perl
  libgmp10 libgnutls-deb0-28 libhogweed4 libhtml-parser-perl libhtml-tagset-perl libhttp-date-perl libhttp-message-perl libicu55
  libimport-into-perl libindirect-perl libio-html-perl libio-stringy-perl libldap-2.4-2 liblexical-sealrequirehints-perl
  liblist-moreutils-perl liblog-message-perl liblog-message-simple-perl liblua5.1-0 liblwp-mediatypes-perl libmagic1 libmodule-build-perl
  libmodule-implementation-perl libmodule-pluggable-perl libmodule-runtime-perl libmodule-signature-perl libmoo-perl libmoox-handlesvia-perl
  libmro-compat-perl libmultidimensional-perl libnamespace-autoclean-perl libnamespace-clean-perl libnettle6 libnghttp2-14 libp11-kit0
  libpackage-constants-perl libpackage-stash-perl libpackage-stash-xs-perl libpadwalker-perl libparams-classify-perl libparams-util-perl
  libparams-validate-perl libpath-tiny-perl libpod-latex-perl libpod-markdown-perl libpod-readme-perl librole-tiny-perl libsasl2-2
  libsasl2-modules libsasl2-modules-db libsoftware-license-perl libsqlite3-0 libssl1.0.2 libstrictures-perl libsub-exporter-perl
  libsub-exporter-progressive-perl libsub-identify-perl libsub-install-perl libsub-name-perl libtasn1-6 libterm-ui-perl libtext-soundex-perl
  libtext-template-perl libtimedate-perl libtry-tiny-perl libtype-tiny-perl libtype-tiny-xs-perl libunicode-utf8-perl liburi-perl
  libvariable-magic-perl libxml2 mime-support openssl perl perl-modules rename sgml-base ssl-cert xml-core
Suggested package[illegible]
  www-browser apa[illegible]
  libsasl2-modules[illegible]dal
  libdevel-stacktrace-perl libwww-perl ca-certificates perl-doc libterm-readline-gnu-perl libterm-readline-perl-perl make libb-lint-perl
  libcpanplus-dist-build-perl libcpanplus-perl libfile-checktree-perl libobject-accessor-perl sgml-base-doc openssl-blacklist debhelper
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils file libalgorithm-c3-perl libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
  libarchive-extra[illegible]l libcgi-pm-perl
  libclass-c3-perl[illegible]n-meta-perl
  libdata-optlist-perl libdata-perl-perl libdata-section-perl libdevel-caller-perl libdevel-globaldestruction-perl libdevel-lexalias-perl
  libencode-locale-perl libexpat1 libexporter-tiny-perl libfcgi-perl libffi6 libfile-slurp-perl libgdbm3 libgetopt-long-descriptive-perl
  libgmp10 libgnutls-deb0-28 libhogweed4 libhtml-parser-perl libhtml-tagset-perl libhttp-date-perl libhttp-message-perl libicu55
  libimport-into-perl libindirect-perl libio-html-perl libio-stringy-perl libldap-2.4-2 liblexical-sealrequirehints-perl
  liblist-moreutils-perl liblog-message-perl liblog-message-simple-perl liblua5.1-0 liblwp-mediatypes-perl libmagic1 libmodule-build-perl
  libmodule-implementation-perl libmodule-pluggable-perl libmodule-runtime-perl libmodule-signature-perl libmoo-perl libmoox-handlesvia-perl
  libmro-compat-perl libmultidimensional-perl libnamespace-autoclean-perl libnamespace-clean-perl libnettle6 libnghttp2-14 libp11-kit0
  libpackage-constants-perl libpackage-stash-perl libpackage-stash-xs-perl libpadwalker-perl libparams-classify-perl libparams-util-perl
  libparams-validate-perl libpath-tiny-perl libpod-latex-perl libpod-markdown-perl libpod-readme-perl librole-tiny-perl libsasl2-2
  libsasl2-modules libsasl2-modules-db libsoftware-license-perl libsqlite3-0 libssl1.0.2 libstrictures-perl libsub-exporter-perl
  libsub-exporter-progressive-perl libsub-identify-perl libsub-install-perl libsub-name-perl libtasn1-6 libterm-ui-perl libtext-soundex-perl
  libtext-template-pe[illegible]iburi-perl
  libvariable-magic-p[illegible]
0 upgraded, 114 newly installed, 0 to remove and 1 not upgraded.
Need to get 23.8 MB of archives.
After this operation, 97.9 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Free Resco Cloud Webinar

Get run through all the solutions Resco Cloud has to offer and who benefits from which.

resco.net

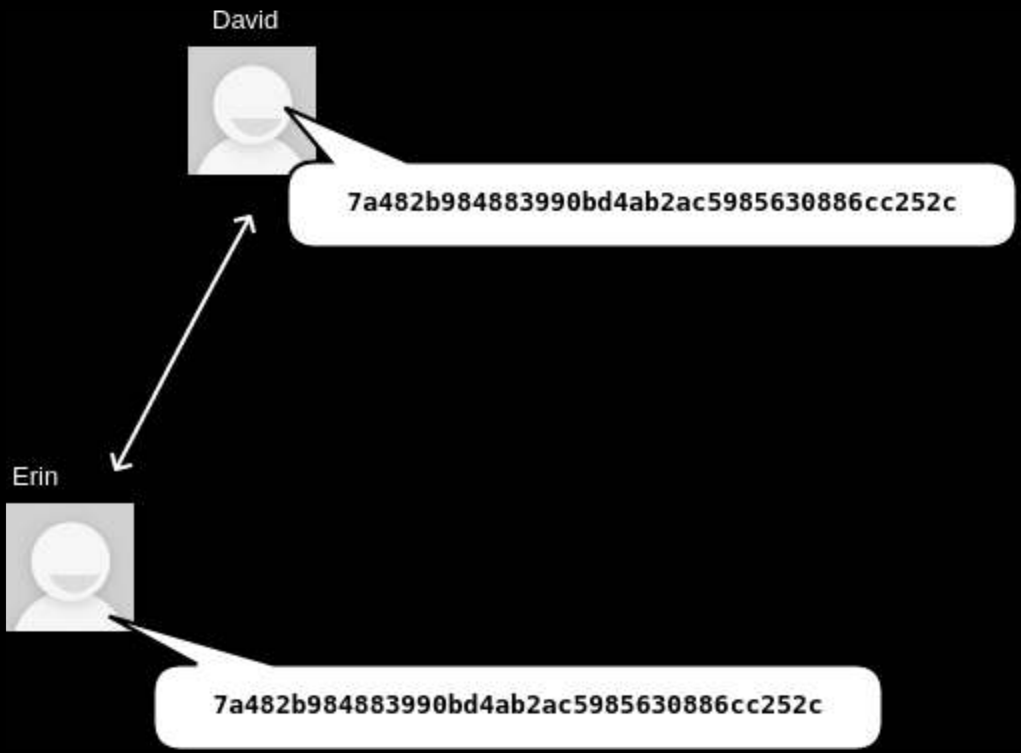
We have a problem.

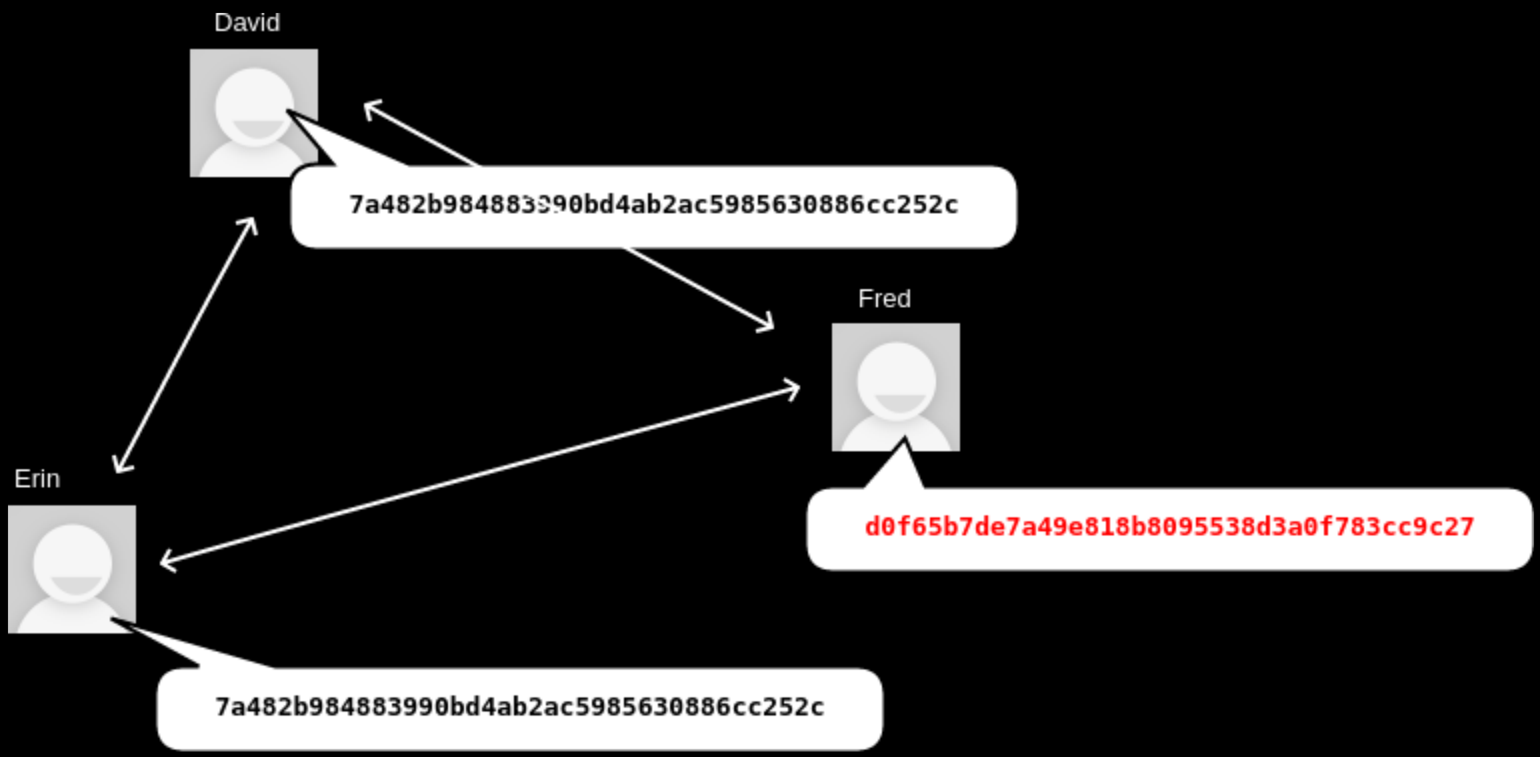
Solution?

1. Start with the same source
2. Ensure builds always have identical results
3. Compare results

David

7a482b984883990bd4ab2ac5985630886cc252c


David
7a482b984883990bd4ab2ac5985630886cc252c
Erin
7a482b984883990bd4ab2ac5985630886cc252c



David

7a482b984883990bd4ab2ac5985630886cc252c

Fred

d0f65b7de7a49e818b8095538d3a0f783cc9c27

Erin

7a482b984883990bd4ab2ac5985630886cc252c

How does this help?

Alice → Blackmail will be uncovered

Bob → Compromise detected

Carol → Tampered laptop will be discovered

Reduces incentive to attack in the first place

"Builds with the same dependencies"... ✖

"Reliable" builds... ✖

Identical build results

Wait…

Dictionary/hash/database ordering

Parallelism in builds

Timestamps

Build paths

Non-deterministic file ordering

Users, groups, `umask`, environment variables, etc.

No doubt, it is a difficult endeavour

And after all that effort...
what do we get?

Minimal diffs on "deliberate" changes

Cache ratio — save time, money & CO_2

Remove really unused build-dependencies

Finds bugs!

Random characters in manpages?

```
-This manual page documents the usageoof WikipediaFS.
+This manual page documents the usage of WikipediaFS.
```

```
memcpy(&buf[1], &buf[2], strlen(buf)-1);
```

```
memcpy(3): The memory areas must not overlap
```

```
- memcpy(&buf[1], &buf[2], strlen(buf)-1);
+ memmove(&buf[1], &buf[2], strlen(buf)-1);
```

UB in docbook-to-man for i386: https://bugs.debian.org/842635

https://sources.debian.org/src/docbook-to-man/1%3A2.0.0-45/debian/patches/0010-Prevent-undefined-behaviour-in-memcpy-parameter-over.patch/

Debian & Reproducible Builds

We have been working in making Debian build reproducibly since 2013

"Torture test"

Time & date

Hostname & domain name

Filesystem (`disorderfs`)

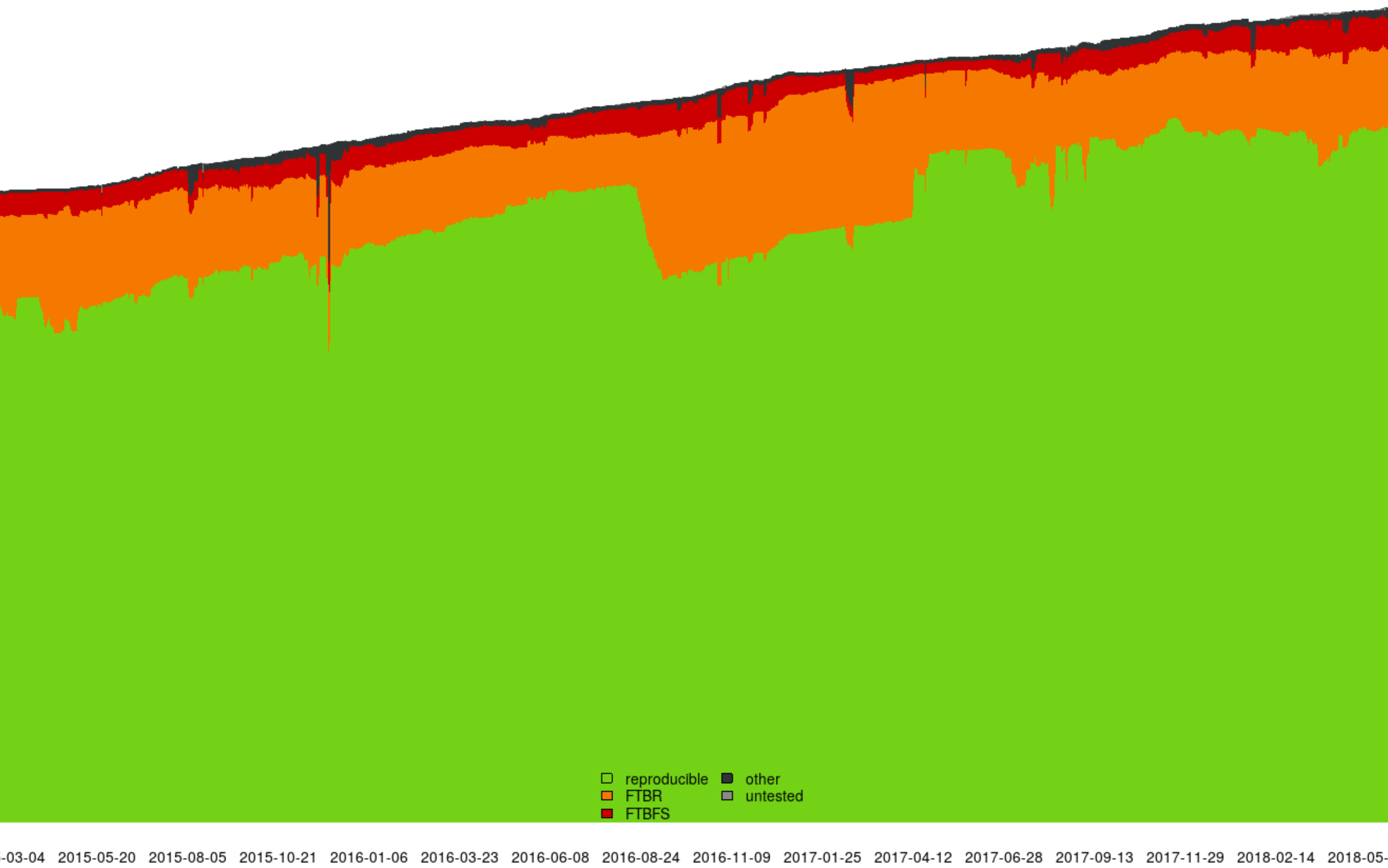
Timezone & locale

`uid` & `gid`

Kernel & CPU type

First rebuild in 2013	24% packages reproducible
March 2018	93% packages reproducible

Reproducibility status for packages in 'unstable' for 'amd64'



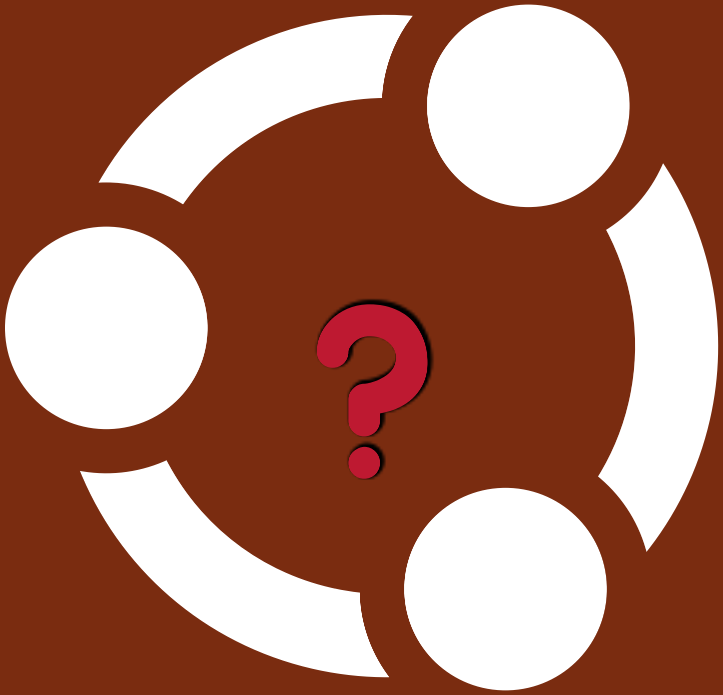
Beyond Debian…

coreboot, Fedora, LEDE, OpenWRT, NetBSD, FreeBSD, Archlinux, Qubes, F-Droid, NixOS, Guix, Meson, etc.

Other projects using "Debian"'s testing framework

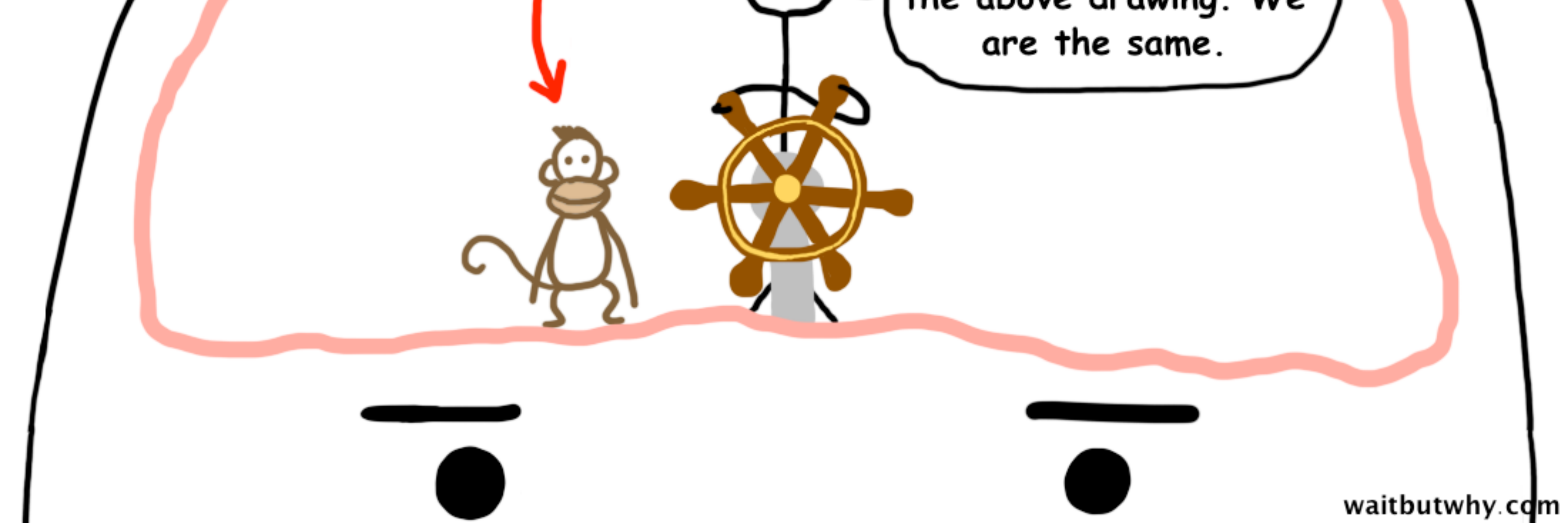
Reproducible Builds summits (Athens, Berlin, Paris, Marrakech, Venice, Hamburg)

And Ubuntu...



I tried rebuilding mantic…

or… I really wanted to! I swear!



Nevertheless, at least I tried with just `main`...

Tot packages in main	2407
packages that I somehow managed to lose	17
packages that were too annoying	13
Tot built packages	2377
Tot reproducible packages	2275 (95.7%)
Tot **UN**reproducible packages	58 (2.4%)
Tot FTBFS packages	44 (1.9%)

About actually rebuilds and verification

Because this is what actually matters: **buildinfos**

```
Format: 1.0
Source: libeatmydata
Binary: eatmydata eatmydata-udeb libeatmydata1 libeatmydata1-dbgsym
Architecture: amd64
Version: 131-1
Checksums-Md5:
 2aa285ab834acf7bf81278be8e78aeb2 6172 libeatmydata1-dbgsym_131-1_amd64.deb
 e9ec9b65e45f3d22eaf583116bcc45d1 6980 libeatmydata1_131-1_amd64.deb
Checksums-Sha1:
 13cfc33f2473c3e12299e7572b97fcd4358e861e 6172 libeatmydata1-dbgsym_131-1_amd64.deb
 144cb89d17e7767ddc6daf1263737d2ae38e75f6 6980 libeatmydata1_131-1_amd64.deb
Checksums-Sha256:
 7a06d1b47fcc7f4784affea446b6100dc72d2a96f25137c4bcdf90ce737032ef 7472 eatmydata_131-1_all.deb
 f3eeadb78571b0373ef3e4624d84536a7c7865e55c879445e53087b8fefaacca 6172 libeatmydata1-dbgsym_131-1_amd64.deb
 183de8aeaec90241574ca570500b7cdbb2662d508907974d2cadf42c03251d4d 6980 libeatmydata1_131-1_amd64.deb
Build-Origin: Debian
Build-Architecture: amd64
Build-Date: Wed, 01 Nov 2023 11:10:37 +0000
Build-Path: /build/libeatmydata-131
Installed-Build-Depends:
 autoconf (= 2.71-3),
 automake (= 1:1.16.5-1.3),
 autopoint (= 0.21-13),
 autotools-dev (= 20220109.1),
 base-files (= 13),
 base-passwd (= 3.6.1),
 bash (= 5.2.15-2+b6),
...
 sysvinit-utils (= 3.08-1),
 tar (= 1.34+dfsg-1.2),
 usr-is-merged (= 37),
 usrmerge (= 37),
 util-linux (= 2.39.2-5),
 xz-utils (= 5.4.4-0.1),
 zlib1g (= 1:1.2.13.dfsg-3)
Environment:
 DEB_BUILD_OPTIONS="parallel=4"
 DPKG_GENSYMBOLS_CHECK_LEVEL="4"
 LANG="C"
 LC_ALL="C"
 LC_TIME="en_US.UTF-8"
 LD_LIBRARY_PATH="/usr/lib/libeatmydata"
 SOURCE_DATE_EPOCH="1693822961"
```

SBOM?

https://bugs.launchpad.net/launchpad/+bug/1686242

Thank you Simon Quigley!

Q & A

Get involved!

Visit:	`reproducible-builds.org`

Subscribe:	`lists.reproducible-builds.org`
	`→ rb-general`

Follow:	**@ReproBuilds** on ~~Twitter~~X
Join:	`#reproducible-builds` (on OFTC)

Thanks!

Reproducible
Builds

mapreri@ubuntu.com
mattia@mapreri.org
mattia@debian.org
mattia@reproducible-builds.org

mapreri.org
reproducible-builds.org