GNU Mes – Full Source Bootstrap

janneke@gnu.org

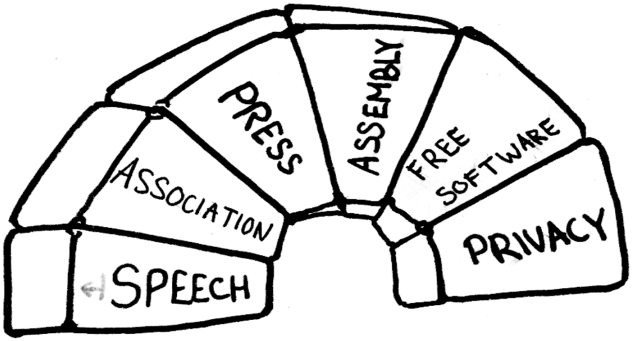
FOSDEM'21

2021-02-07

Outline

1. Introduction
2. Reproducibility
3. Bootstrappability
4. Freedom
5. Thanks

Full Source Bootstrap: Why?



Full Source Bootstrap: GNU Mes

GNU Mes

- A Scheme interpreter written in ~5,000LOC of simple C.
- A C compiler written in Scheme.
- Built on LISP: eval/apply, the Maxwell Equations of Software.

The Holy Grail: Stage0's hex0 => Mes

The holy grail of bootstrappability will be connecting mes to hex0.
– Carl Dong, Chaincode Labs

Full Source Bootstrap: WE DID IT!!!

Full Source Bootstrap: hex0 => M2-Planet => GNU Mes

GNU Mes

- A Scheme interpreter written in ~5,000LOC of simple C, or M2.
- A C compiler written in Scheme.
- Built on LISP: eval/apply, the Maxwell Equations of Software.

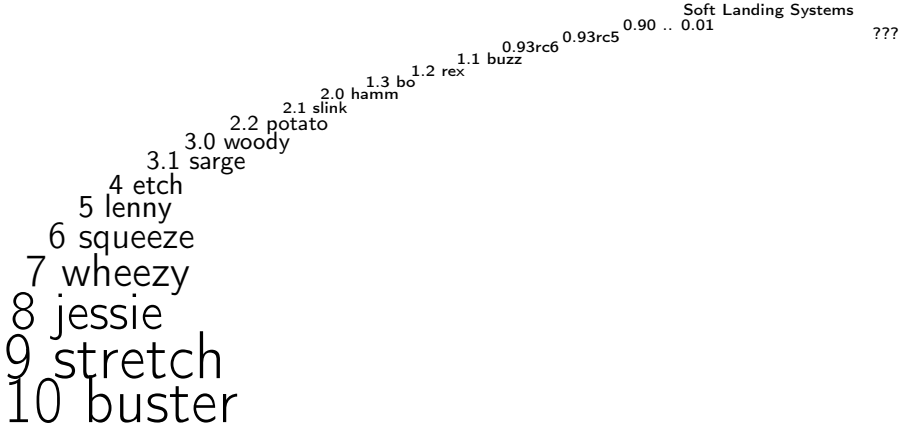
Ken Thompson

TURING AWARD LECTURE

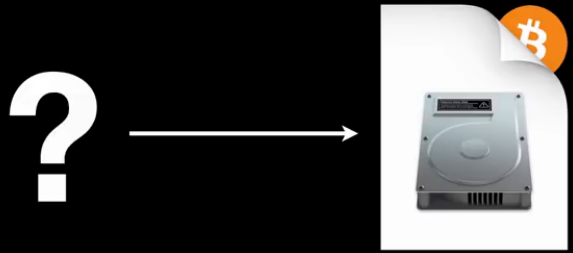
Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

Journey to the Source?

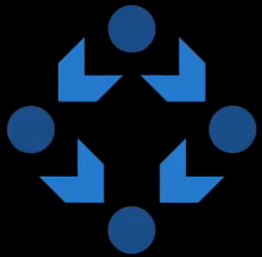


As time goes on we will expire the binary packages for old releases. Currently we have binaries for squeeze, lenny, etch, sarge, woody, potato, slink, hamm and bo available, and only source code for the other releases. – www.debian.org/distrib/archive



Bitcoin Build System Security

Carl Dong, Chaincode Labs



Reproducible Builds

What is a Bootstrap?

Impossible task: pull yourself up on your boot straps

Software: to create your first: kernel, shell, C compiler, ...

How to Bootstrap: An Old Recipe...

Recipe for yoghurt: Add yoghurt to milk – Anonymous

How to Bootstrap: Create your second GCC

Traditional recipe: like yoghurt

. . . and done!

We’re Reproducible!

We’re Reproducible!

We’re Reproducibly Malicious

Reproducibility **is not enough**

Reproducibility
Clean source code

is not enough

Guix

Pronounced *Geeks*

NLnet Foundation

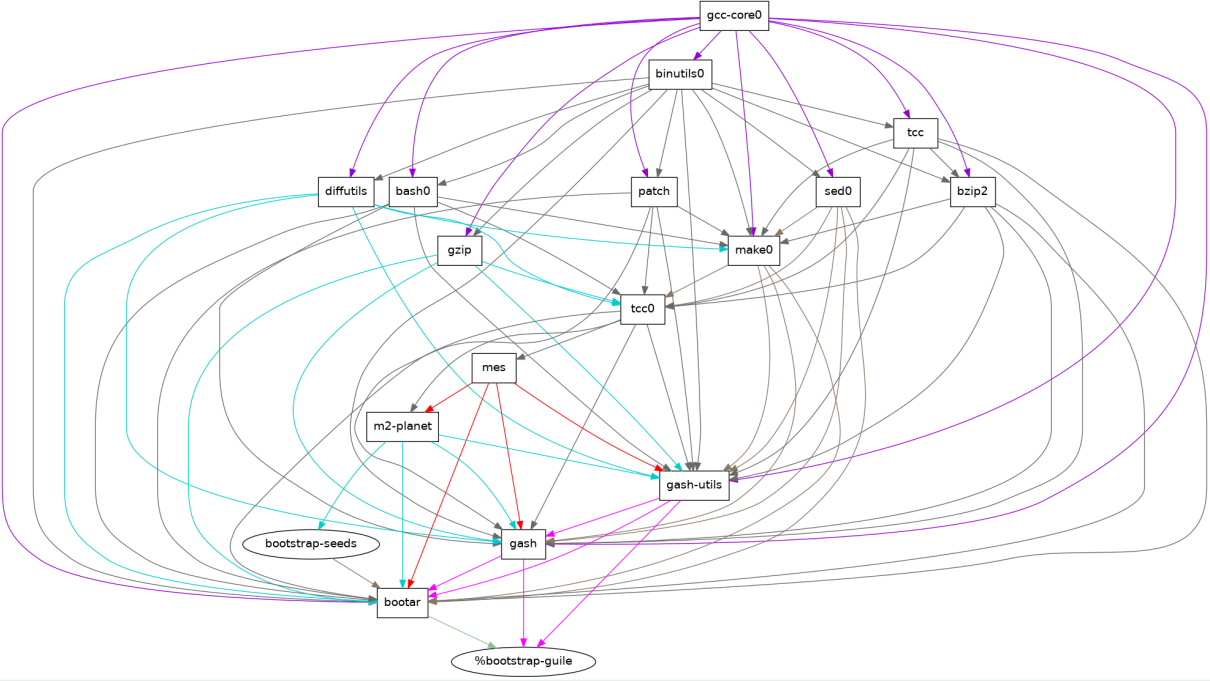
WE DID IT! We did what?

Adapt Mes and Mes C Library for M2-Planet

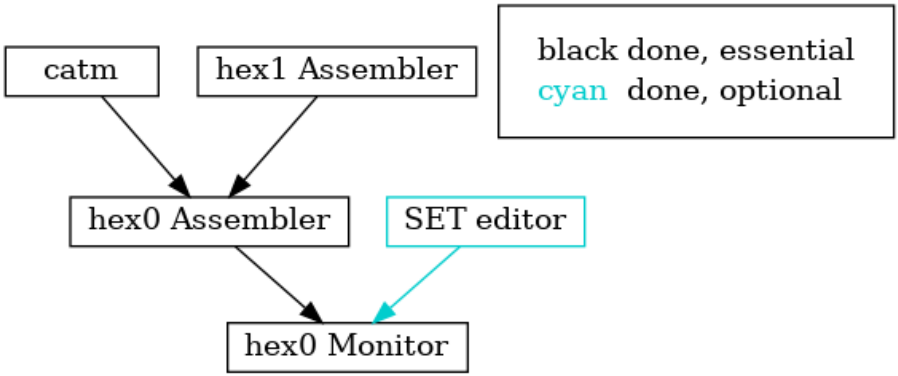
- #define FOO => ...; #if BAR => ...; CAR (x) => x->car
- remove global and static array data
- foo.bar => foo->bar
- rewrite pointer arithmetic
- rewrite garbage collector
- mature M2-Planet
- ...

Integrate Full Source Bootstrap

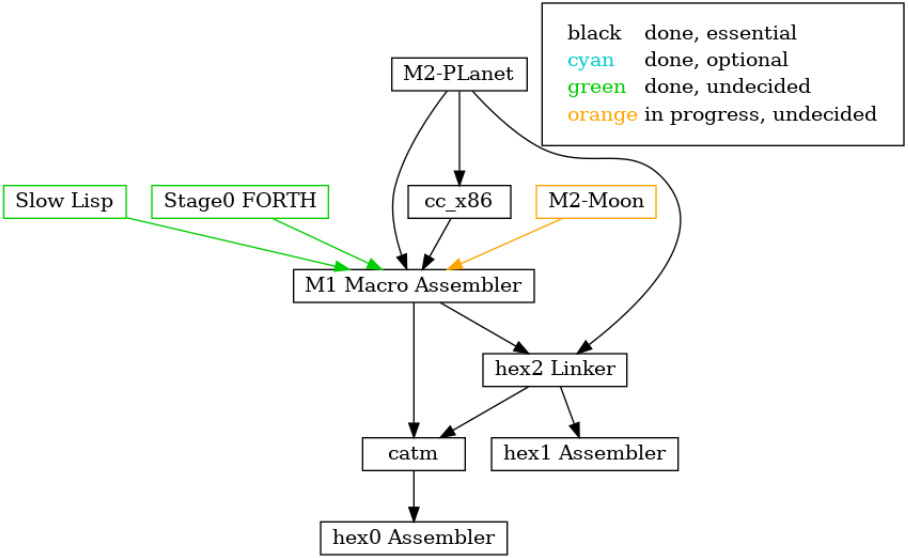
- package M2-Planet
- remove (dependency on) bootstrap seeds
- ...


gcc-core0
binutils0
tcc
diffutils
bash0
patch
sed0
bzip2
gzip
make0
tcc0
mes
m2-planet
gash-utils
bootstrap-seeds
gash
bootar
%bootstrap-guile

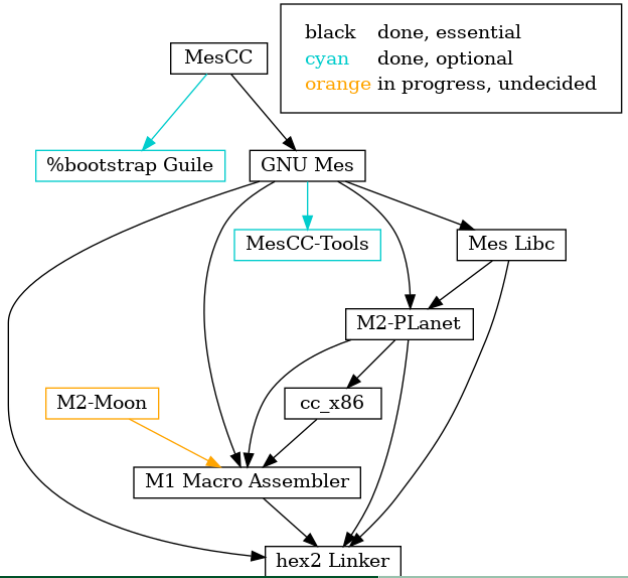
Full Source Bootstrap: Stage 0



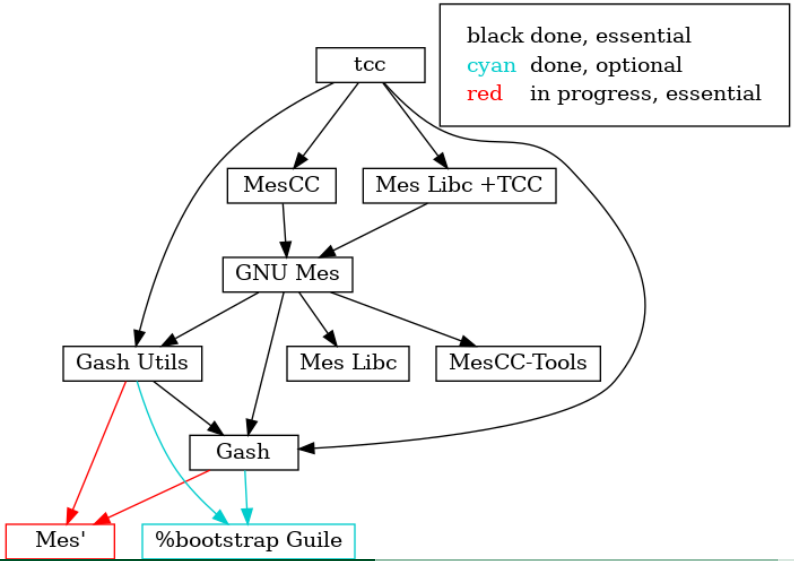
Full Source Bootstrap: Stage 1



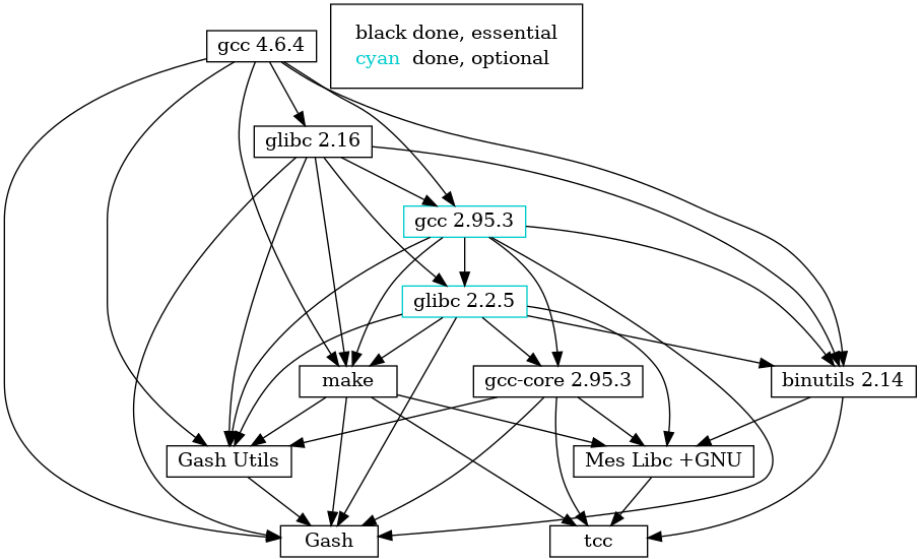
Full Source Bootstrap: Stage 2



Full Source Bootstrap: Stage mes



Full Source Bootstrap: Stage mesboot



Long path: Full Source Bootstrap

- 500+ MB: no bootstrap
- 252 MB: GNU Guix System v1.0
- 145 MB: Reduced Binary Seed
  - master branch
  - ~~GCC~~, ~~GLIBC~~, ~~Binutils~~
  - + MesCC-Tools, + Mes
- 57 MB: Scheme-only
  - wip-bootstrap branch
  - ~~Awk~~, ~~Bash~~, ~~Bzip2~~, ~~GNU Core Utilities~~, ~~Grep~~, ~~Gzip~~, ~~Make~~, ~~Patch~~, ~~Sed~~, ~~Tar~~, and ~~XZ~~.
  - + Gash (source only!)
- 357 bytes: Full Source
  - ~~MesCC-Tools~~, ~~Mes~~
  - + Stage0: 357 bytes (x86)

Trusted Computing Base

- Source code
- Binary seeds
- Guix System
- Linux
- Guix's Childhurds (Hurd in VM)

What's Next?

wip-full-source-bootstrap

- release mes-0.24
- update and merge

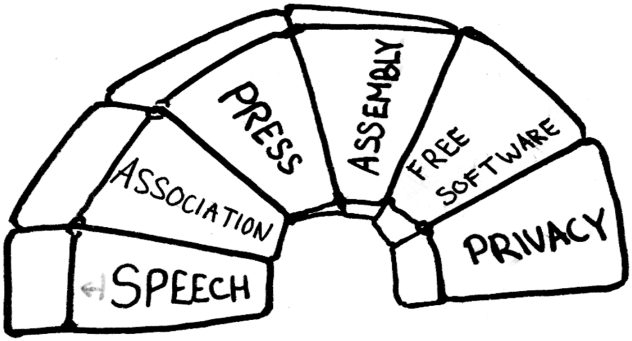
wip-arm-bootstrap

- the bootstrap: currently stuck at gawk-mesboot0
- release mes-0.23
- update and merge

RISC-V

- remove gcc-2.95 from the bootstrap
- port RISC-V extensions to gcc-4.6

Free Software as a Human Right



Freedom of Computing

Free Software == Freedom of Computing

- Inspect source => Free Software
- Binary matches source? => Reproducible builds
- Toolchain compromised? => Bootstrappable builds
- Hardware trustable? => DDC, free hardware

Moving target: Are we losing GCC?

June 12, 2014

GCC 4.7.4, the final "bootstrappable", already a huge download

August 3rd, 2016

GCC 4.9.4 released, as of 4.8 requires C++03 to bootstrap

May 18, 2020

GCC moved away from C++03 and now needs to C++11 to bootstrap

Contemplate: What is happening?

It just doesn't feel right
– Vagrant Cascadian, Debian developer

Joy of Source

Vulnerability to a trusting trust attack is a symptom of an unauditable or missing bootstrap story. – janneke

Choices: More control, or less control?

raise bootstrappable awareness

to take back control over our computing, or

keep doing what we're doing

and watch the erosion of our computing freedoms.

Thanks

- Carl Dong
- Danny Milosavljevic
- David Terry
- Jeremiah Orians
- Ludovic Courtès
- Matt Wette
- Pjotr Prins
- Rutger van Beusekom
- Timothy Sample
- Vagrant Cascadian

Want to join?

You can help

- raise awareness
- make core GNU packages bootstrappable again
- GCC (c++!), GNU Libc (python?!)
- reduced bootstrap NixOS, Debian
- port MesCC to the Hurd, FreeBSD
- retweet/toot `@janneke_gnu janneke@octodon.social`

Connect

- irc freenode.net #bootstrappable #guix
- mail bug-mes@gnu.org guix-devel@gnu.org
- git https://git.savannah.gnu.org/git/mes.git
- web bootstrappable.org