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?

(C) 2014 Richard Stallman and others, CC-BY 3.0
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 of bootstrappability will be connecting mes to hex0.
– Carl Dong, Chaincode Labs
Full Source Bootstrap: WE DID IT!!!
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.
Reflexions 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.
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
What is a Bootstrap?

Impossible task: pull yourself up on your boot straps

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

source + ?? = binary
Recipe for yoghurt: Add yoghurt to milk – Anonymous
How to Bootstrap: Create your second GCC

Traditional recipe: like yoghurt

... and done!
Pour milk
Add yoghurt
We’re Reproducible!
Add evil yoghurt
We’re Reproducible!
We’re Reproducibly Malicious
Reproducibility is not enough
Reproducibility is not enough, clean source code is not enough.
Guix

Pronounced Geeks
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
- ...

janneke@gnu.org (FOSDEM’21)
Full Source Bootstrap: Stage 1

- Black: done, essential
- Cyan: done, optional
- Green: done, undecided
- Orange: in progress, undecided

Diagram:
- Slow Lisp → M2-PLanet
- Slow Lisp → Stage0 FORTH
- M2-PLanet → cc_x86
- M2-Moon → cc_x86
- M1 Macro Assembler
- hex2 Linker
- catm → hex0 Assembler
- hex1 Assembler
Full Source Bootstrap: Stage 2

- **black**: done, essential
- **cyan**: done, optional
- **orange**: in progress, undecided

Diagram:

- MesCC
- %bootstrap Guile
- GNU Mes
- MesCC-Tools
- Mes Libc
- M2-PLanet
- M2-Moon
- cc_x86
- M1 Macro Assembler
- hex2 Linker
Full Source Bootstrap: Stage mesboot

- gcc 4.6.4
- glibc 2.16
- glibc 2.2.5
- gcc 2.95.3
- make
- gcc-core 2.95.3
- binutils 2.14
- Gash Utils
- Gash
- Mes Libc + GNU
- tcc

black done, essential cyan done, optional
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
- finish the bootstrap: currently stuck at glibc-mesboot0 (2.2.5)
- 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

(C) 2014 Richard Stallman and others, CC-BY 3.0
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*
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