GNU Mes – Bootstrapping GNU

janneke@gnu.org

Libre Planet ’20

2020-03-15
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.
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.
500+ MB: no bootstrap
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 + ?? = GCC

gcc binary
Recipe for yoghurt: Add yoghurt to milk – Anonymous
How to Bootstrap: Create your second GCC

Traditional recipe: like yoghurt

source + GCC = binary - 1 = GCC binary

... and done!
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
Guix
Pronounced Geeks
Long path: Scheme-only 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!)
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)
Vulnerability to a trusting trust attack is a symptom of an unauditable or missing bootstrap story. – Janneke
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
  - XZ-only => .GZ tarballs (thank you: sed, coreutils!)
  - GCC (c++!), GNU Libc (python?!)  
- reduced bootstrap NixOS, Debian
- port MesCC to the Hurd, FreeBSD
- retweet/toot @janneke GNU janneke@octodons.
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