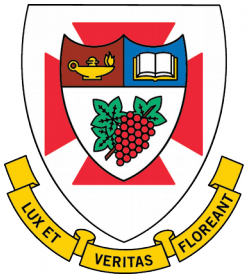
Re-Bootstrapping the Free World

Mark Jenkins
BCSc (honours)

mark@markjenkins.ca

1DEE 93CC DA25 F8A3 F9E3
57A9 A8F8 6493 AA4D B1FB

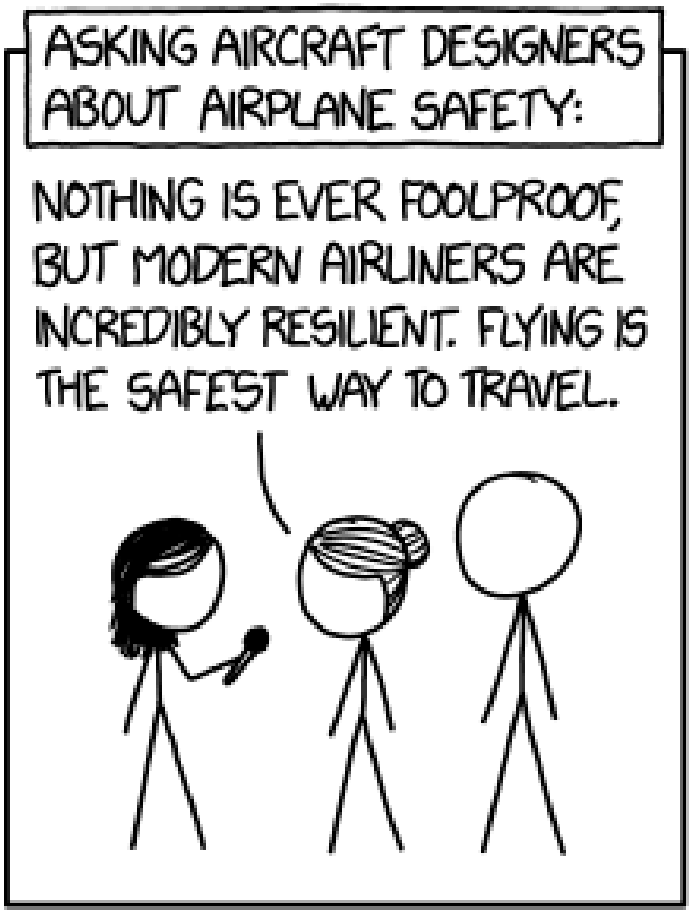
About me: Affiliations (All opinions mine)



THE UNIVERSITY OF WINNIPEG

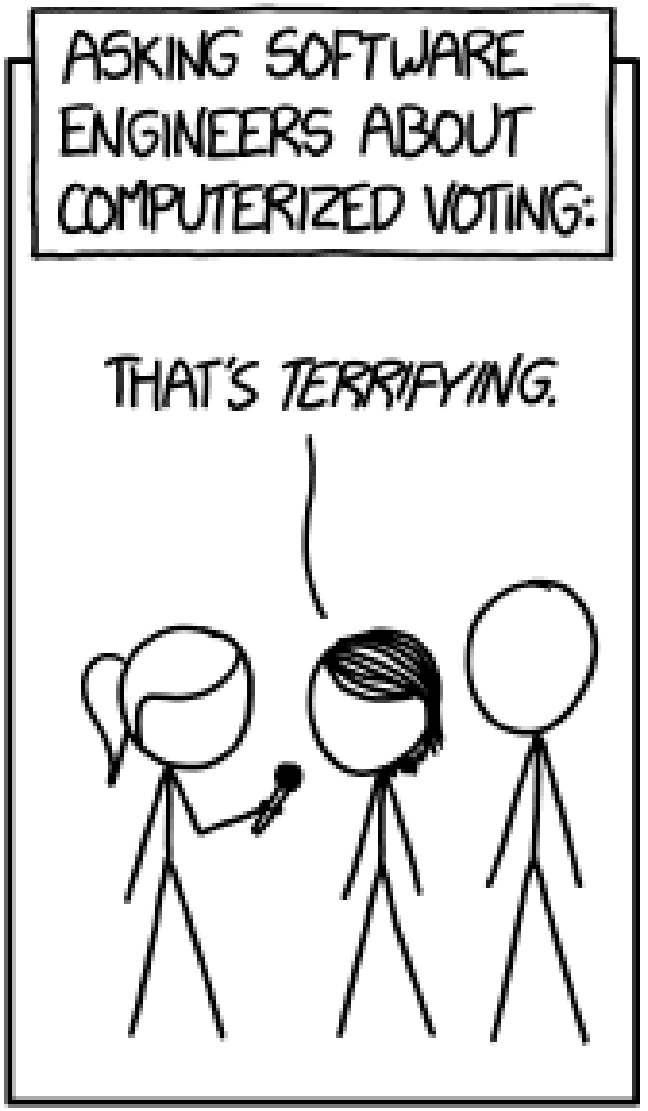
PARIT WORKER CO-OP

https://xkcd.com/2030/



ASKING BUILDING ENGINEERS ABOUT ELEVATOR SAFETY:

ELEVATORS ARE PROTECTED BY MULTIPLE TRIED-AND-TESTED FAILSAFE MECHANISMS. THEY'RE NEARLY INCAPABLE OF FALLING.


ASKING SOFTWARE ENGINEERS ABOUT COMPUTERIZED VOTING:
THAT'S TERRIFYING.


WAIT, REALLY?
DON'T TRUST VOTING SOFTWARE AND DON'T LISTEN TO ANYONE WHO TELLS YOU IT'S SAFE.
WHY?
I DON'T QUITE KNOW HOW TO PUT THIS, BUT OUR ENTIRE FIELD IS BAD AT WHAT WE DO, AND IF YOU RELY ON US, EVERYONE WILL DIE.


THEY SAY THEY'VE FIXED IT WITH SOMETHING CALLED "BLOCKCHAIN."
AAAAA!!!
WHATEVER THEY SOLD YOU, DON'T TOUCH IT.
BURY IT IN THE DESERT.
WEAR GLOVES.

Wired 2018-10-25
I BOUGHT USED VOTING MACHINES ON EBAY FOR $100 APIECE.
WHAT I FOUND WAS ALARMING -- Brian Varner

Image source Boing Boing

N>=2 users, 1 computer

Raising the bar: some voting machine criteria

- Published FLOSS
- Scrutineer witnessed software load
- Supervised after load
  (Trusted Platform Module [TPM] attestation during operation and as part of final output may be too late)

Software load option #1

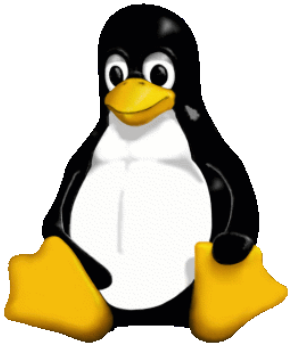
- Reproducible build
- Read-only install media passed around for read-back by scrutineer

Software load option #2

- Firmware is a short bootstrap ROM
- Bootstrap ROM verified by some external means

Software load option #2 -- continued

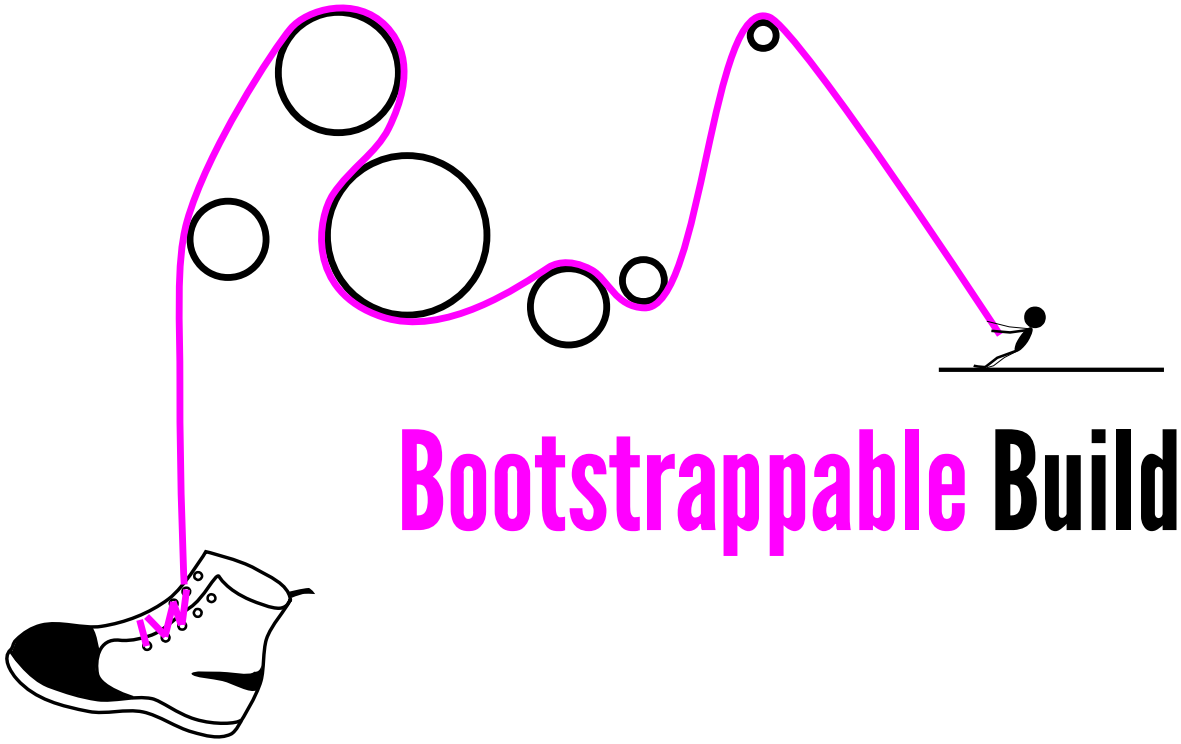
- Software loaded by bootstrap process
- Each bootstrap phase can report cryptographic hash of next stage source before compiling/interpreting it



linux-4.14.78.tar.xz

SHA256:
f4da4dc0f079e420e1c1b8c713
12eaa5415b08be847aa224a61
d8af6a6e74c6c

https://bootstrappable.org



Jan Nieuwenhuizen
https://gitlab.com/janneke/

https://archive.fosdem.org/2017/schedule/event/guixsdbootstrap/
https://www.youtube.com/watch?v=7NFD_9d7J3Q

GNU Mes
https://www.gnu.org/software/mes/
Mutual self-hosting

mes.c  MesCC

- Scheme interpreter written in simple C

  (a good language for writing a portable interpreter that you want to bootstrap)

- C compiler written in scheme

  (a good language for writing a language compiler)

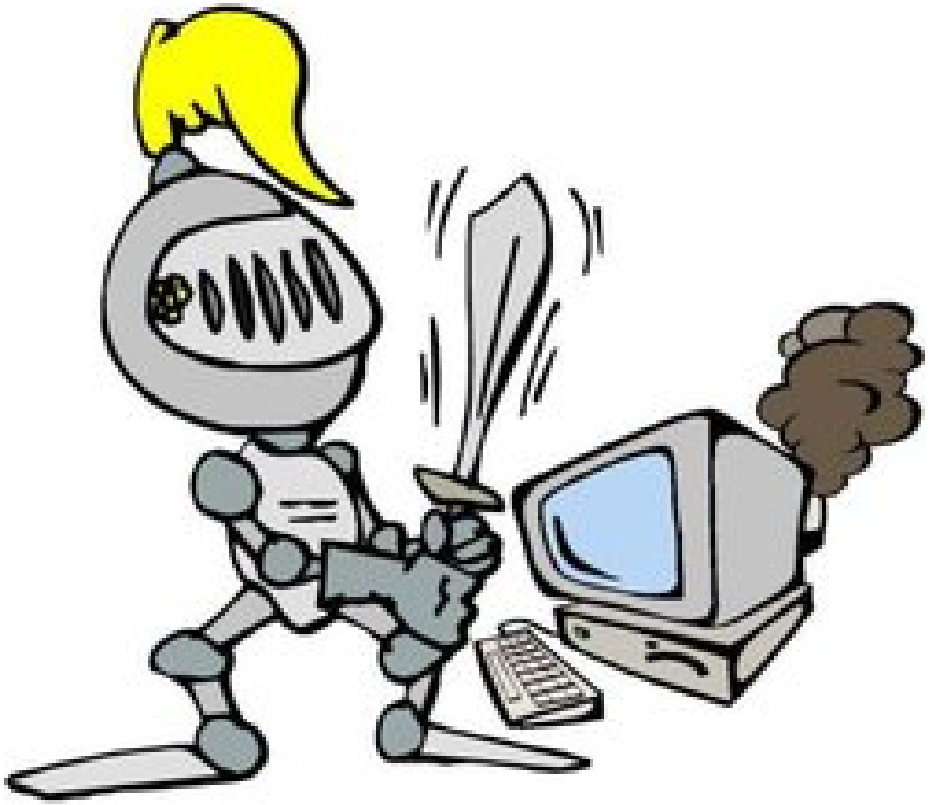
The GNU tripplet

glibc

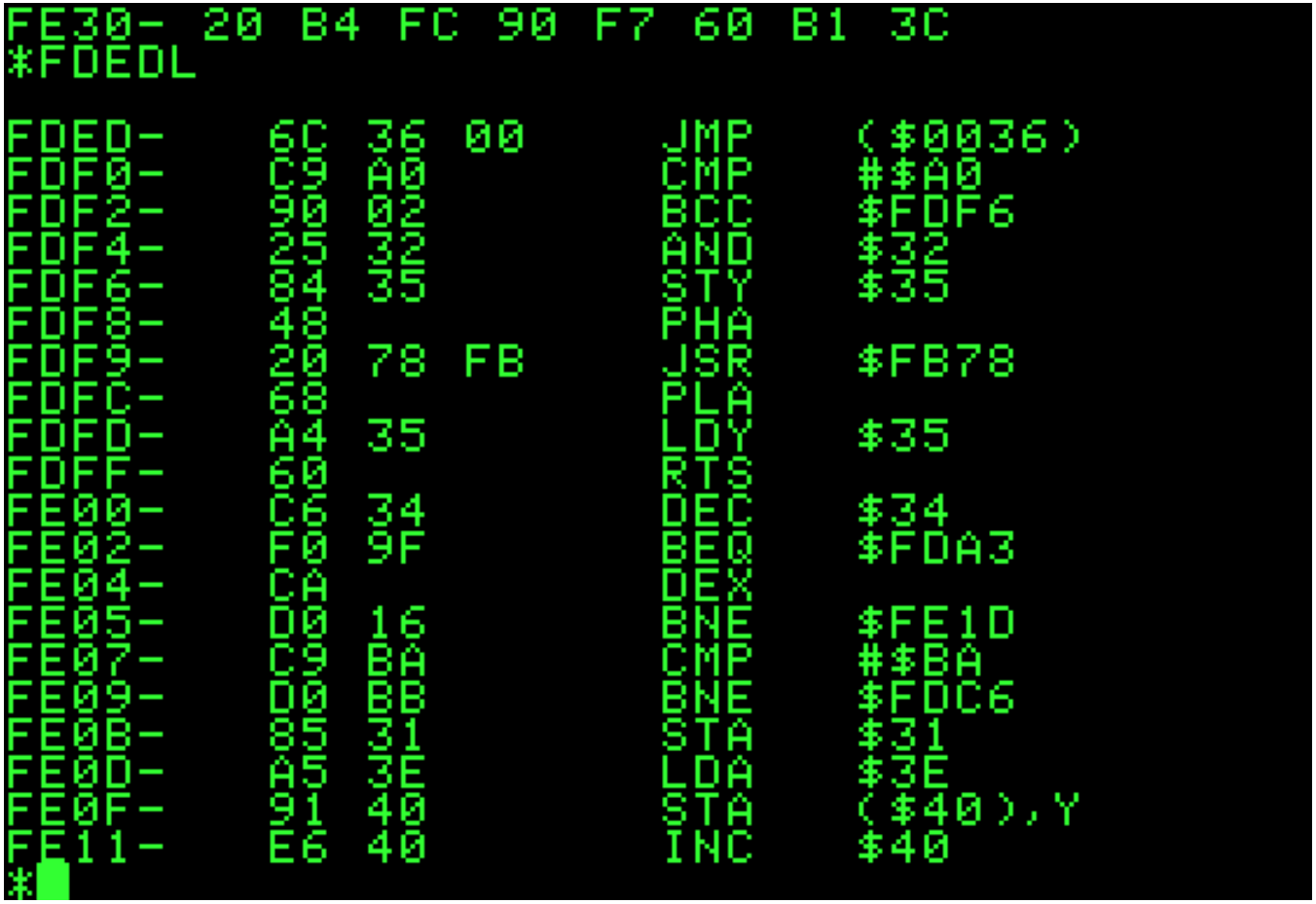
GNU binutils

Jeremiah Orians
https://github.com/oriansj

https://github.com/oriansj/stage0



Stage0 -- Machine code monitor



Stage1

- Hex assemblers of increasing complexity (labels, absolute/relative addressing) (Hex0-Hex2)
- Macro assemblers of increasing complexity (M0, M1, M2)

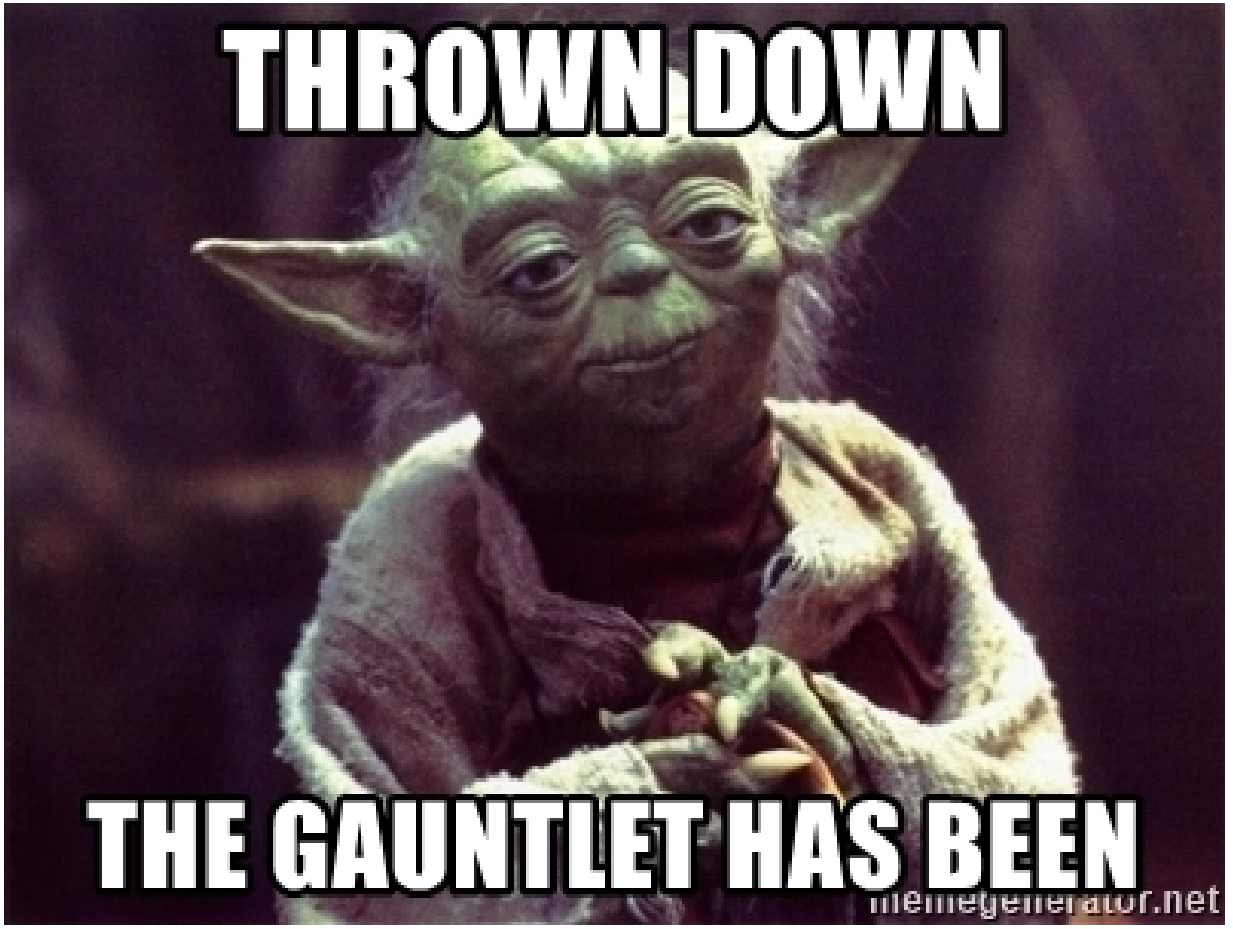
Stage0 + Mes combined progress

- Mes.c (scheme interpreter) output to M1 macro assembler language, free world now bootstrapable with 1M “readable” blob of that M1 code. Much smaller than previous blob of GNU triplet (gcc, glibc, binutils) binary build.
- Subset of C compiler written in macro assembler (M2Planet, Orians), rewrites of Mes.c into simplified C variant in progress (mes-m2)

FORTH

“Because a great many people stated FORTH would be an ideal bootstrapping language the time and effort was put forth....ultimately it was determined, Assembly was preferable as the underlaying architecture wasn’t total garbage.

It now sits waiting for any FORTH programmer who wishes to prove FORTH is a real bootstrapping language.”


THROWN DOWN
THE GAUNTLET HAS BEEN
memegenerator.net


KEEP CALM
THE GAUNTLET
HAS BEEN
THROWN
DOWN

Self programable with FORTH

Other in-person cases for bootstraping a software load for problems of N>=2 users, 1 computer

- Wright-Andresen (N=2) Problem
- Authenticated data feed for smart contracts (“oracle”), but without relying on Intel secure enclaves (SGX) as town-crier.org does.
  (to avoid depletion, requires a periodic meetup and re-bootstraping of a fleet of additional battery backed oracle nodes)

Other cases page 2

Privacy sensitive shared tenancy hosting co-op where hosting customers are secured against co-location host. Requires one-time meetup for each new piece of hosting gear group bootstrap/load and new TPM keys. Combine with a fleet of battery backed, periodically refreshed bootstraped oracles that validate TPM attestation before unlocking rest of boot process (alternative to Golem cryptocurrency's future reliance on Intel secure enclaves [SGX])

?

Happy Hacking