Foundries.io

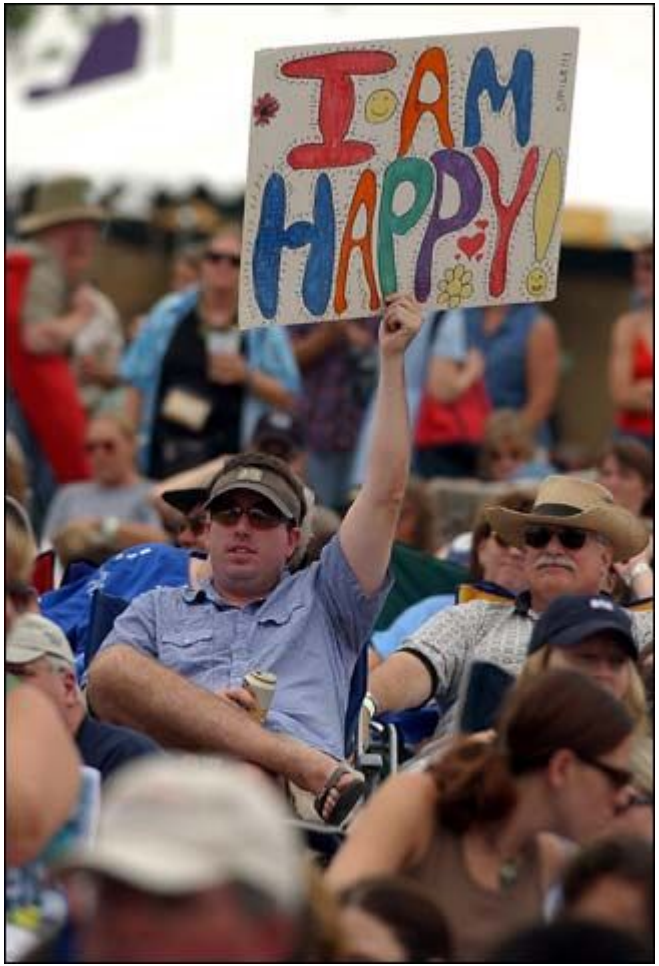
Aktualizr-lite: Be secure and never use /bin/dd again

Andy Doan andy@foundries.io

Background / About Me

There’s a better way to live

A picture from ACL 2003



Background

Almost all ways to update embedded devices suck the joy out of your life

/bin/dd is just a giant sinkhole of despair

I Know What I’m Talking About

Because I’ve Failed So Much

- LAVA - SD Cards and later the SD Mux
- Canonical UTAH and Ubuntu Phone Work
- Some that never got that far

About Update Systems

There are two ways people are doing updates:

- A/B partitioning - double the disk space
- OSTree - “git for filesystems”

How to do it securely varies. Probably GPG-ish stuff

The Update Framework (TUF) - is an industry standard

Uptane extends TUF and is used by the automotive industry

“But you don’t sound that smart”

About Aktualizr

It’s the one project that does Ostree and Uptane

It’s open source!

They open sourced their back end services as well!

It’s gaining pretty decent and (TUF level security) support for Docker

It’s in cars - this is a serious project with extremely high stakes involved.

But what about ostree+gpg?

TUF was created in part because GPG is insufficient.

- Handles lost signing key (key rotation)
- Downgrade attacks
- Other complex stuff hackers use

Why aktualizr-lite?

Uptane is hard (both technically, client side, and server side)

Uptane tells devices what to be

In many cases that’s simply: “always up-to-date”

Making this decision simplifies things

But what about “campaigns”

Safely rolling something out is the biggest problem

TUF “Targets” can include custom metadata. We added a concept of “tags”. Ie “premerge”, “qa”, “release”.

“*But we already have our own secure OTA system*”

No You Don’t

If you’ve rolled your own, then you’re only safe until Matthew Garrett gets 2 hours with your product.

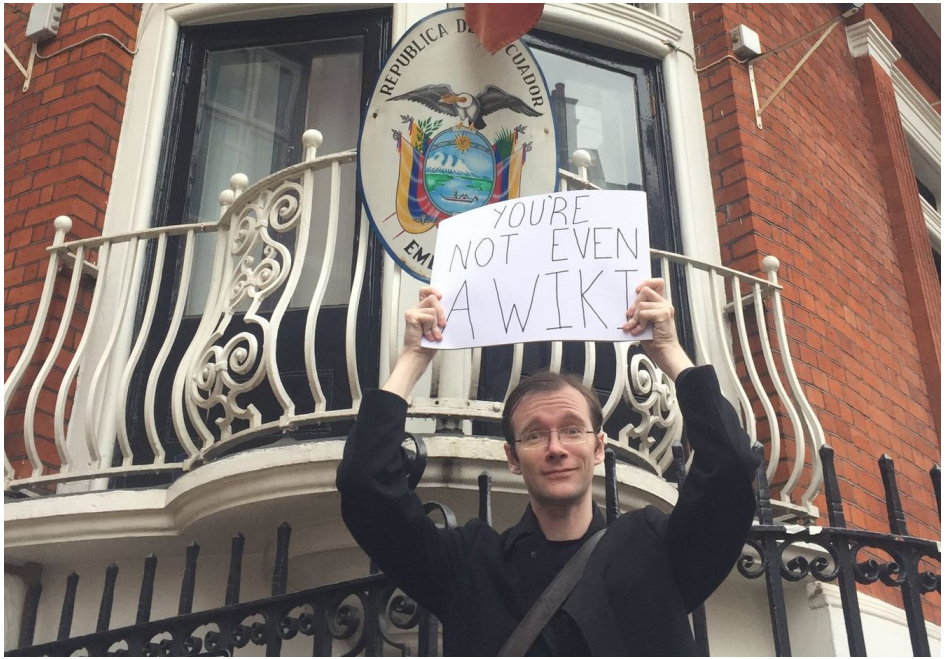


Image Source: Wikipedia

“*But what about the backend?*”

Its Open Too!

https://github.com/advancedtelematic/ota-community-edition

https://github.com/foundriesio/ota-compose

https://foundries.io/insights/2018/07/12/ota-part-4/

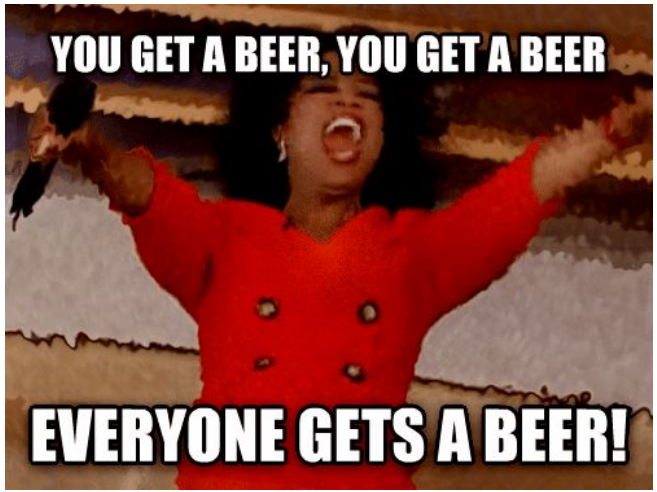


Image Source: gfycat.com

What does it look like?

https://api.foundries.io/ota/repo/andy-corp/api/v1/user_repo/targets.json

And How Does Docker Fit In

Docker Apps are added to TUF Repo

Each platform Target includes the Docker App targets applicable to it

How to try it out

Hard Way

Update your OE build with meta-updater and our patches:

https://github.com/foundriesio/meta-lmp/tree/master/recipes-sota/aktualizr

Easier Way

Grab one of our images and use “dd” one last time:

https://github.com/foundriesio/lmp-manifest/releases

Thank you

Resources

Blog Series:

- https://foundries.io/insights/2018/07/12/ota-part-4/
- https://foundries.io/insights/2018/08/09/ota-api/

Docker Apps Idea: https://github.com/advancedtelematic/aktualizr/pull/1189

aktualizr-lite Idea:

- https://github.com/advancedtelematic/aktualizr/issues/1056
- https://github.com/advancedtelematic/aktualizr/pull/1107