Asfaload: Securing downloads from the internet

Bauduin Raphaël

www.asfaload.com

2025-02-04

The problem

Downloads from the internet

We download a lot of software from the internet (Github Releases, Docker images, ...)

The problem

Downloads from the internet

We download a lot of software from the internet (Github Releases, Docker images, ...)

No authenticity checks

But authenticity check is often impossible (checksums are not authenticity checks)

A problem causing the problem

We need a solution for median humans

Existing authentication system are not usable by mere mortals

Asfaload proposal

A usable solution

Propose an **easy to use**, **multi-sig**, file **authentication** system to secure downloads from the internet

Asfaload proposal

A usable solution

Propose an **easy to use**, **multi-sig**, file **authentication** system to secure downloads from the internet

Wanna safely download something?

Only the URL of the file to be downloaded is needed!

Asfaload proposal

A usable solution

Propose an **easy to use**, **multi-sig**, file **authentication** system to secure downloads from the internet

Wanna safely download something?

Only the URL of the file to be downloaded is needed!

Wanna publish something?

- Just ensure you publish a checksums file
- We will help with handling signatures

Building on the shoulders of giants

We reuse existing blocks

- git
- minisign/signify (OpenBSD origins)
- Let's encrypt inspiration: authenticate at repo level

Building on the shoulders of giants

We reuse existing blocks

- git
- minisign/signify (OpenBSD origins)
- Let's encrypt inspiration: authenticate at repo level

And we only adds missing pieces

- Maintain a checksums mirror, augmented
- Define some json glue

Building on the shoulders of giants

We reuse existing blocks

- git
- minisign/signify (OpenBSD origins)
- Let's encrypt inspiration: authenticate at repo level

And we only adds missing pieces

- Maintain a checksums mirror, augmented
- Define some json glue

We build an open solution

- All FOSS
- Transparent: Make it easy to integrate
- Provide reference implementation of downloader

Asfaload Checksums Mirror

Central piece of solution

- additional copy of checksums
- keeps list of repo signers

Asfaload Checksums Mirror

Central piece of solution

- additional copy of checksums
- keeps list of repo signers

Transparent

- git fast-forward only
- auditable
- checker scripts

Mirror utility

Even without signatures

- independent source of checksums
- protects against updates after file was mirrored

Step by Step

Starting small

- Repo-agnostic solution
  - start with github
  - expand to other services and self-hosting
  - including container images

File signatures

Coming soon

- File signing
  - just define configs and processes
  - reuse cryptography from minisign

Threat model

We do NOT protect against

- compromised account registered with Asfaload
- build process compromises

Threat model

We do NOT protect against

- compromised account registered with Asfaload
- build process compromises

We protect against

- File update in existing releases
- Unauthorised file publication
- Release by compromised account (multi-sig)
- Publisher key compromise (multi-sig)

In active development

Help shape the solution

- Give us your critical feedback
- Join us a test publishers
- Use `asfald` our downloader today to validate checksums

In active development

Help shape the solution

- Give us your critical feedback
- Join us a test publishers
- Use `asfald` our downloader today to validate checksums

Use our Github Actions

- Notify us of your new releases
- Use our asfald Action in your own workflows

Join us

Contact info

- https://www.asfaload.com
- https://github.com/asfaload
- https://github.com/asfaload/spec
- https://mastodon.social/@asfaload
- https://bsky.app/profile/asfaload.bsky.social
- raphael@...