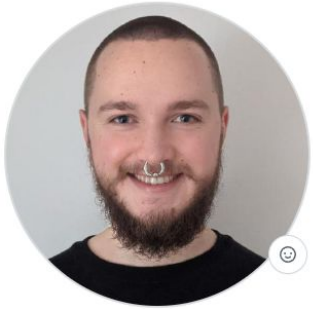
Go in the Nix ecosystem

status quo,
vulnerability scanning, and
experiments towards a next-gen builder

graphic @egonelbre

meta

- Paul Meyer
- GitHub @katexochen
- Mastodon @katexochen@infosec.exchange
- security software engineer @edgelesssys
- nixpkgs maintainer/committer
- part of the nixpkgs Go team
- author of @hmnews@techhub.social



Paul Meyer
katexochen

Dependency management in Go

- go.mod declares minimal required versions of module dependencies
  - Released, versioned, and distributed together
- go.sum contains cryptographic hashes of modules
  - Not a lockfile, can contain multiple versions
  - Hashes incompatible with nix
- Minimal Version Selection
  - Deterministic algorithm to select versions
  - Only one version of a dependency is selected
- List dependencies after MVS (build list): `go list -m all`
- go.dev/ref/mod

```
module github.com/suzuki-shunsuke/pinact

go 1.23.4

require (
    github.com/google/go-cmp v0.6.0
    github.com/google/go-github/v68 v68.0.0
    github.com/hashicorp/go-version v1.7.0
    github.com/mattn/go-colorable v0.1.14
    github.com/sirupsen/logrus v1.9.3
    github.com/spf13/afero v1.12.0
    github.com/suzuki-shunsuke/gen-go-jsonschema v0.1.0
    github.com/suzuki-shunsuke/logrus-error v0.1.4
    github.com/urfave/cli/v2 v2.27.5
    golang.org/x/oauth2 v0.25.0
    gopkg.in/yaml.v3 v3.0.1
)

require (
    github.com/bahlo/generic-list-go v0.2.0 // indirect
    github.com/buger/jsonparser v1.1.1 // indirect
    github.com/cpuguy83/go-md2man/v2 v2.0.5 // indirect
    github.com/google/go-querystring v1.1.0 // indirect
    github.com/invopop/jsonschema v0.12.0 // indirect
    github.com/mailru/easyjson v0.7.7 // indirect
    github.com/mattn/go-isatty v0.0.20 // indirect
```

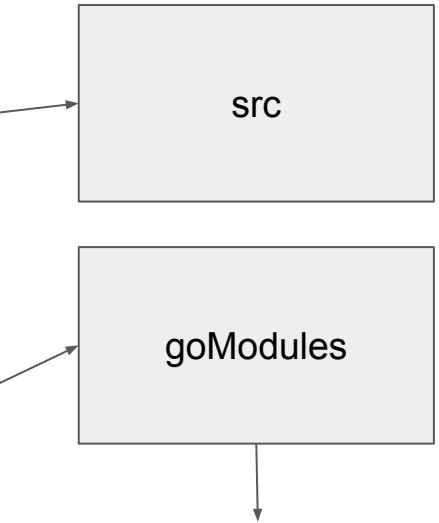
```
github.com/urfave/cli/v2 v2.27.5 h1:WoHEJLdsXr6dDWoJgMq/CboDmyY/8HMMH1fTECbih+w=
github.com/urfave/cli/v2 v2.27.5/go.mod h1:3Sevf16NykTbInEnD0yKkjDAeZDS0A6bzhBH5hrMvTQ=
github.com/wk8/go-ordered-map/v2 v2.1.8 h1:5h/BUHu93oj4gIdvHHHGsScSTMijfx5PeYkE/fJgbpc=
github.com/wk8/go-ordered-map/v2 v2.1.8/go.mod h1:5nJHM5DyteebpVlHnWMV0rPz6Zp7+xBAnxjb1X5vnTw=
github.com/xrash/smetrics v0.0.0-20240521201337-686a1a2994c1 h1:gEOO8jv9F4OT7lGCjxCBTO/36wtF6j2nSip77qHd4x4=
github.com/xrash/smetrics v0.0.0-20240521201337-686a1a2994c1/go.mod h1:Ohn+xnUBiLI6FVj/9LpzZWtj1/D6lUovWYBkxHVV3aM=
golang.org/x/oauth2 v0.25.0 h1:CY4y7XT9v0cRI9oupztF8AgiIu99L/ksR/Xp/6jrZ70=
golang.org/x/oauth2 v0.25.0/go.mod h1:XYTD2NtWslqkgxebSiOHnXEap4TF09sJSc7H1sXbhtI=
golang.org/x/sys v0.0.0-20220715151400-c0bba94af5f8/go.mod h1:oPkhp1MJrh7nUepCBck5+mAzfO9JrbApNNgaTdGDITg=
golang.org/x/sys v0.6.0/go.mod h1:oPkhp1MJrh7nUepCBck5+mAzfO9JrbApNNgaTdGDITg=
golang.org/x/sys v0.29.0 h1:TPYlXGxvx1MGTn2GiZDhnjPA9wZzZeGKHHmKhHYvgaU=
golang.org/x/sys v0.29.0/go.mod h1:/VUhepiaJMQUp4+oa/7Zr1D23ma6VTLIYjOOTFZPUcA=
golang.org/x/text v0.21.0 h1:zyQAAkrwaneQ066sspRyJaG9VNi/YJ1NfzcGB3hZ/qo=
golang.org/x/text v0.21.0/go.mod h1:4IBbMaMmOPCJ8SecivzSH54+73PCFmPWxNTLm+vZkEQ=
golang.org/x/xerrors v0.0.0-20191204190536-9bdfabe68543/go.mod h1:I/5z698sn9Ka8TeJc9MKroUUfqBBauWjQqLJ2OPfmY0=
gopkg.in/check.v1 v0.0.0-20161208181325-20d25e280405 h1:yhCVgyC4o1eVCa2tZl7eS0r+SDo693bJlVdllGtEeKM=
gopkg.in/check.v1 v0.0.0-20161208181325-20d25e280405/go.mod h1:Co6ibVJAznAaIkqp8huTwlJQCZ016jof/cbN4VW5Yz0=
gopkg.in/yaml.v3 v3.0.0-20200313102051-9f266ea9e77c/go.mod h1:K4uyk7z7BCEPqu6E+C64Yfv1cQ7kz7rIZviUmN+EgEM=
gopkg.in/yaml.v3 v3.0.1 h1:fxVm/GzAzEWqLHuvctI91KS9hhNmmWOoWu0XTYJS7CA=
gopkg.in/yaml.v3 v3.0.1/go.mod h1:K4uyk7z7BCEPqu6E+C64Yfv1cQ7kz7rIZviUmN+EgEM=
```

buildGoModule

```
{
  pet = buildGoModule rec {
    pname = "pet";
    version = "0.3.4";

    src = fetchFromGitHub {
      owner = "knqyf263";
      repo = "pet";
      rev = "v${version}";
      hash = "sha256-Gjw1dRrgM8D3G7v6WIM2+50r4HmTXvx0Xxme2fH9TlQ=";
    };

    vendorHash = "sha256-ciBIR+a1oaYH+H1PcC8cD8ncfJczk1IiJ8iYNM+R6aA=";
```

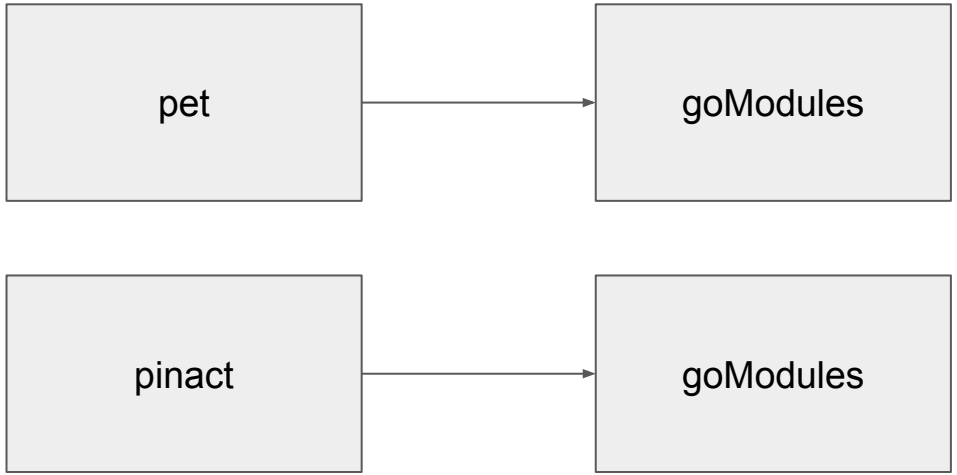
buildGoModule

```
{
  pet = buildGoModule rec {
    pname = "pet";
    version = "0.3.4";

    src = fetchFromGitHub {
      owner = "knqyf263";
      repo = "pet";
      rev = "v${version}";
      hash = "sha256-Gjw1dRrgM8D3G7v6WIM2+50r4HmTXvx0Xxme2fH9TlQ=";
    };

    vendorHash = "sha256-ciBIR+a1oaYH+H1PcC8cD8ncfJczk1IiJ8iYNM+R6aA=";
```




```
github.com/atotto/clipboard v0.1.4
github.com/briandowns/spinner v1.23.1
github.com/chzyer/readline v1.5.1
github.com/fatih/color v1.18.0
github.com/google/go-github v17.0.0+incompatible
github.com/inconshreveable/mousetrap v1.1.0 // indirect
github.com/mattn/go-colorable v0.1.13 // indirect
github.com/mattn/go-isatty v0.0.20 // indirect
github.com/mattn/go-runewidth v0.0.16
```

buildGoModule




```
github.com/rivo/uniseg v0.4.7 // indirect
github.com/stretchr/testify v1.10.0
golang.org/x/sys v0.28.0 // indirect
golang.org/x/text v0.21.0 // indirect
golang.org/x/time v0.8.0 // indirect
```

```
github.com/russross/blackfriday/v2 v2.1.0 // ind
github.com/wk8/go-ordered-map/v2 v2.1.8 // indir
github.com/xrash/smetrics v0.0.0-20240521201337-
golang.org/x/sys v0.29.0 // indirect
golang.org/x/text v0.21.0 // indirect
```

buildGoModule

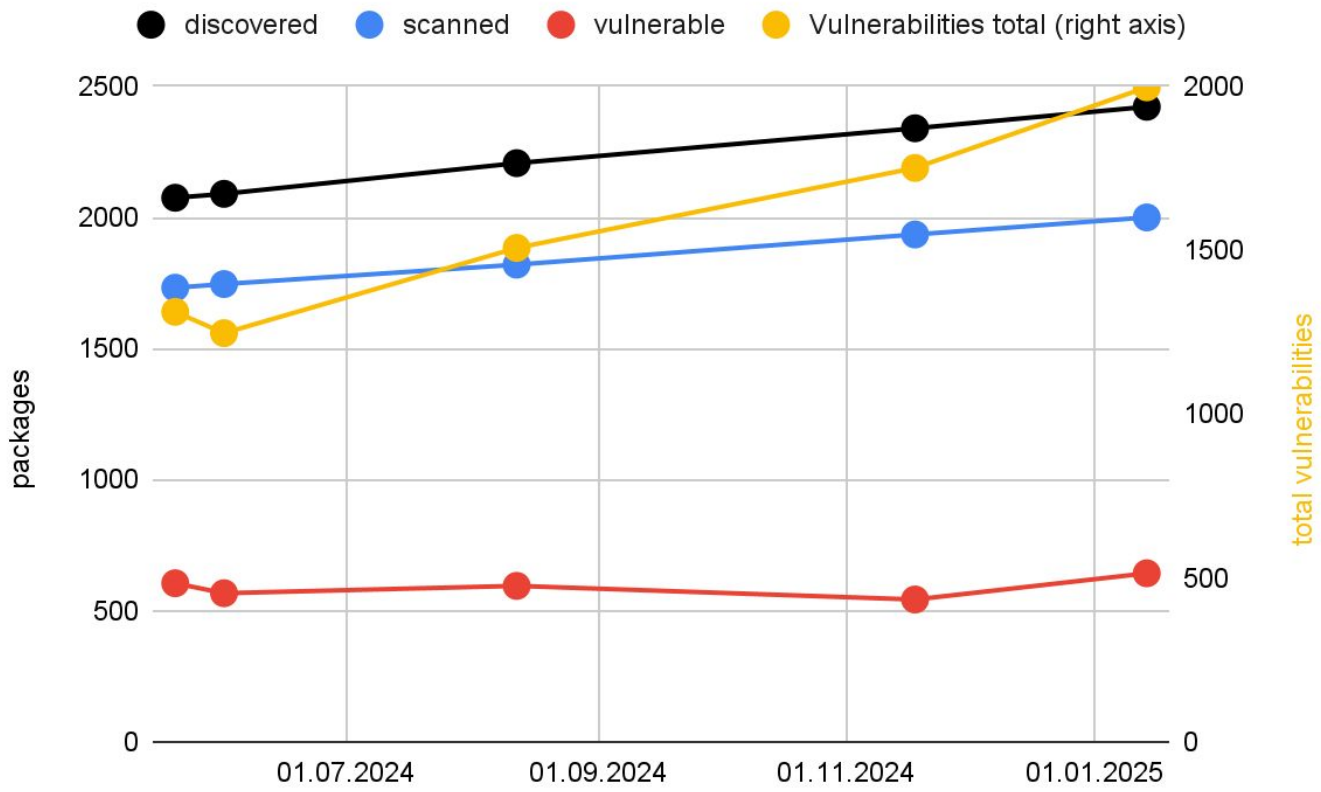
- Bandwidth
- Storage
- No Caching
- No introspection into dependencies in Nix
- No way to easily update dependencies
- No way to patch vulnerabilities

```
github.com/rivo/uniseg v0.4.7 // indirect
github.com/stretchr/testify v1.10.0
golang.org/x/sys v0.28.0 // indirect
golang.org/x/text v0.21.0 // indirect
golang.org/x/time v0.8.0 // indirect

github.com/russross/blackfriday/v2 v2.1.0 // ind
github.com/wk8/go-ordered-map/v2 v2.1.8 // indir
github.com/xrash/smetrics v0.0.0-20240521201337-
golang.org/x/sys v0.29.0 // indirect
golang.org/x/text v0.21.0 // indirect
```

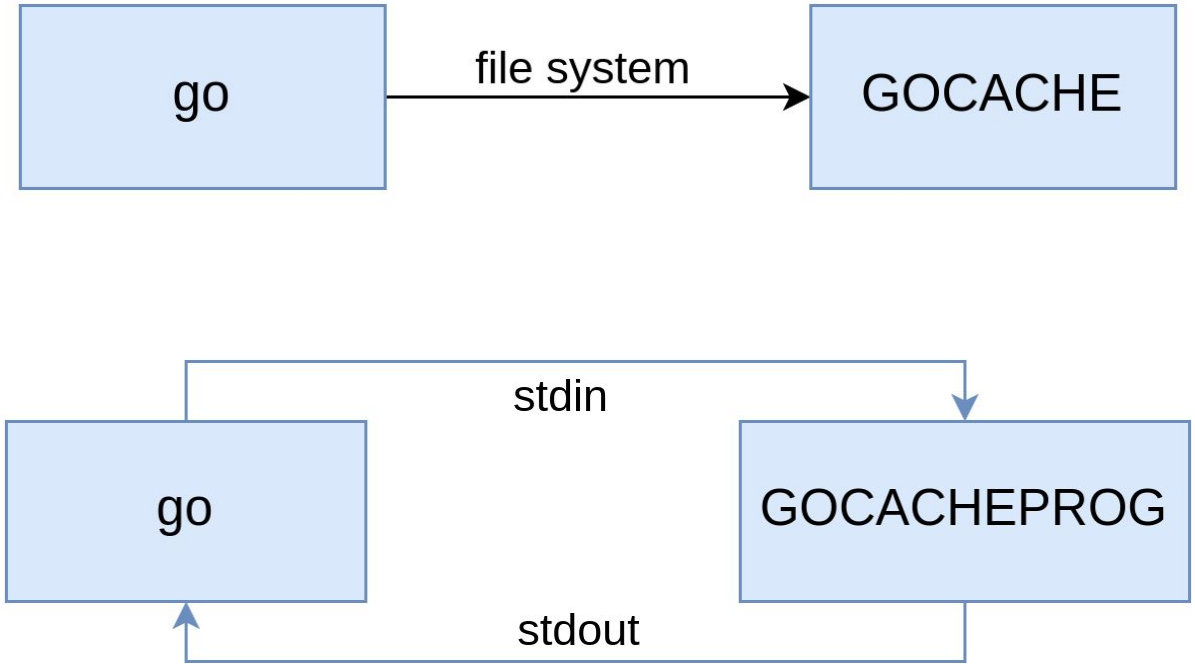
govulncheck-nixpkgs

- govulncheck is the official vulnerability scanning tool for Go
- Uses Go's vulndb
- Checks if vulnerable code is reachable
- Run govulncheck on `src` of packages build with buildGoModule

govulncheck-nixpkgs



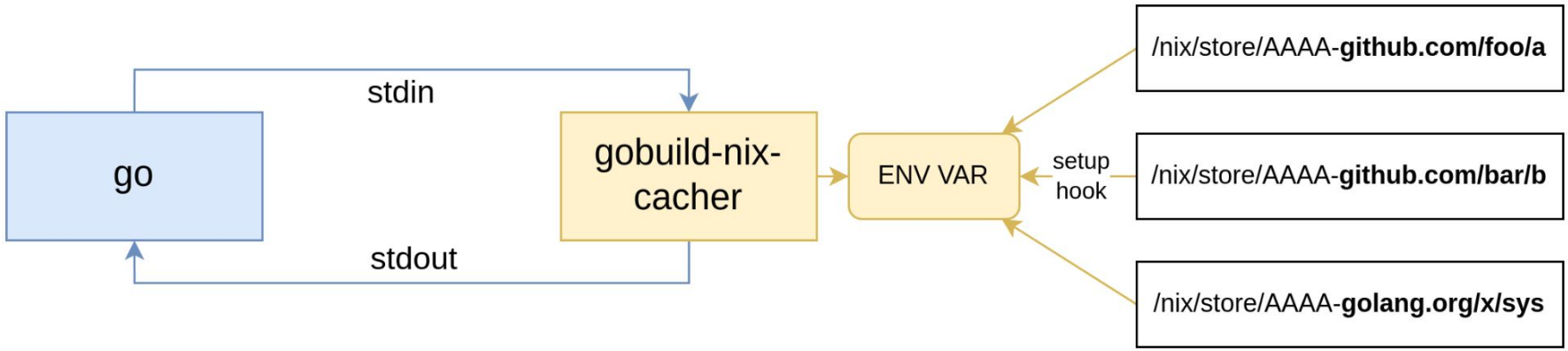
GOCACHEPROG (go 1.24)



gobuild.nix

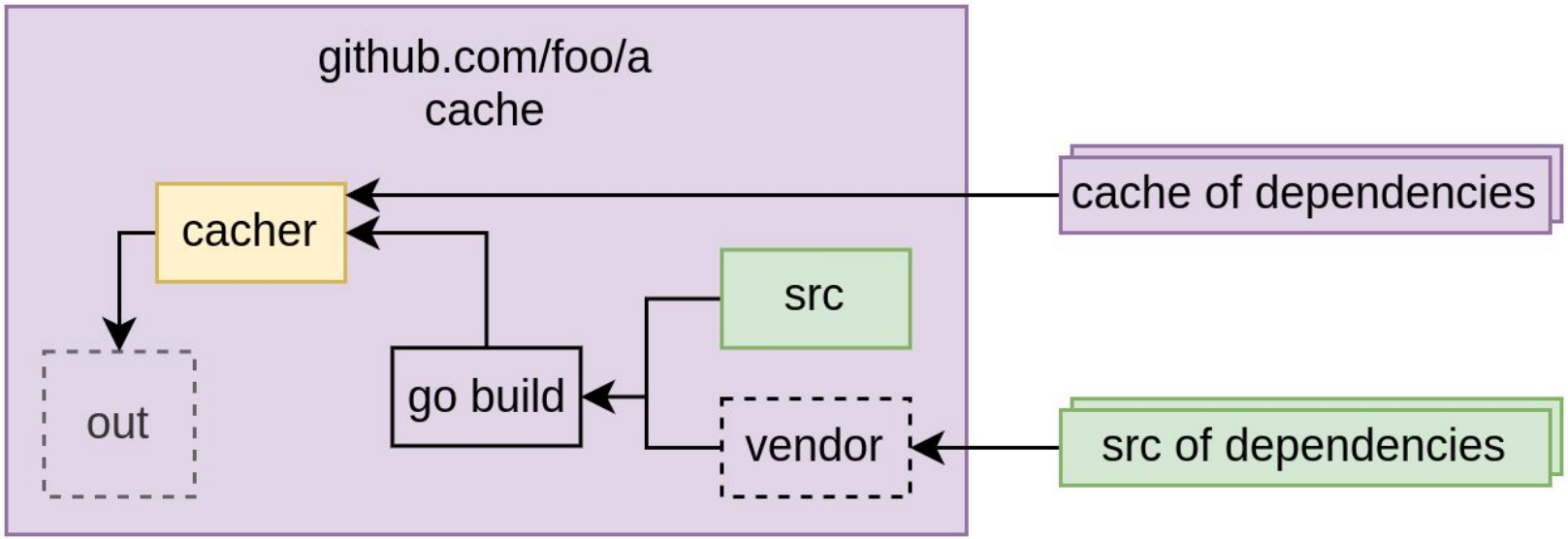
- Next-gen builder for Go
- Use GOCACHEPROG
- Provide a package set of Go dependencies
- Each Go module as one derivation

gobuild.nix: GOCACHEPROG

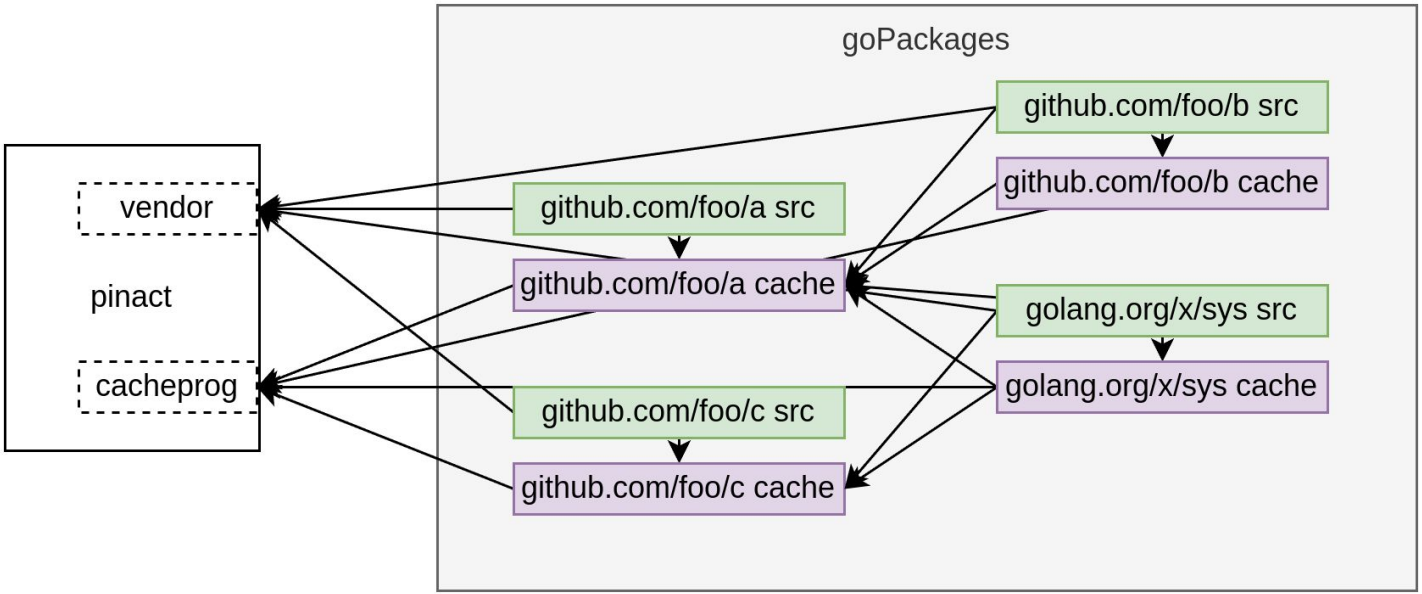


Props to @adisbladis for initial implementation

gobuild.nix at derivation level



gobuild.nix: the package set



Big thanks to @malt3 for continued help implementing this!

gobuild.nix

- Incremental src fetching
- Incremental builds/ caching
- Composability via setup hooks
- Possibility to patch vulnerabilities
- (Maybe) provide a GOPROXY

- Target: nixpkgs
- Status: highly experimental, not usable yet

Looking for people to collaborate on this!

For both

github.com/katexochen/gobuild.nix

and

github.com/katexochen/govulncheck-nixpkgs

Talk to me here or write to @katexochen:matrix.org

Go go Go!

github.com/nix-community/gomod2nix

- fetching dependencies individually, code generation

github.com/numtide/build-go-cache

- build cache for all dependencies in a single derivation, code gen

github.com/dnr/nix-gocacheprog

- GOCACHEPROG, cache outside of nix, impurity