RustPräzi

[rʌstpʁɛˈt͡si:z]

A  to build a  call graph of 

JOSEPH HEJDERUP, MORITZ BELLER, GEORGIOS GOUSIOS

/ @jhejderup, @Inventitech & @gousiosg

TU Delft

FOSDEM 03.02.19

About me

PhD Student @ TU Delft

Working on dependency management problems

Pull request prioritization service

Dependency checkers (like `cargo audit`)

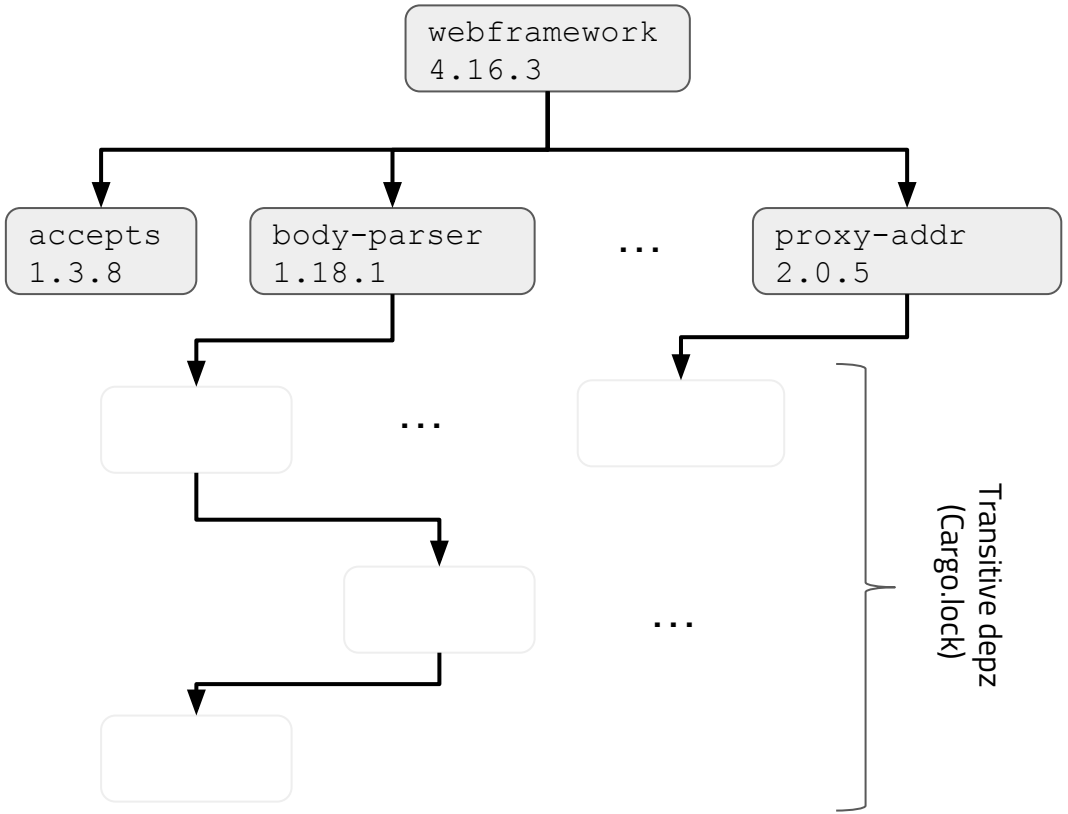
```
[package]
name = “webframework”
version = "4.16.3"

[dependencies]
accepts = "~1.3.5"
body-parser = "1.18.2"
depd = "~1.1.2"
encodeurl = "1.0.2"
escape-html = "~1.0.3"
etag = "1.8.1"
proxy-addr = "~2.0.3"
```

1.3.8

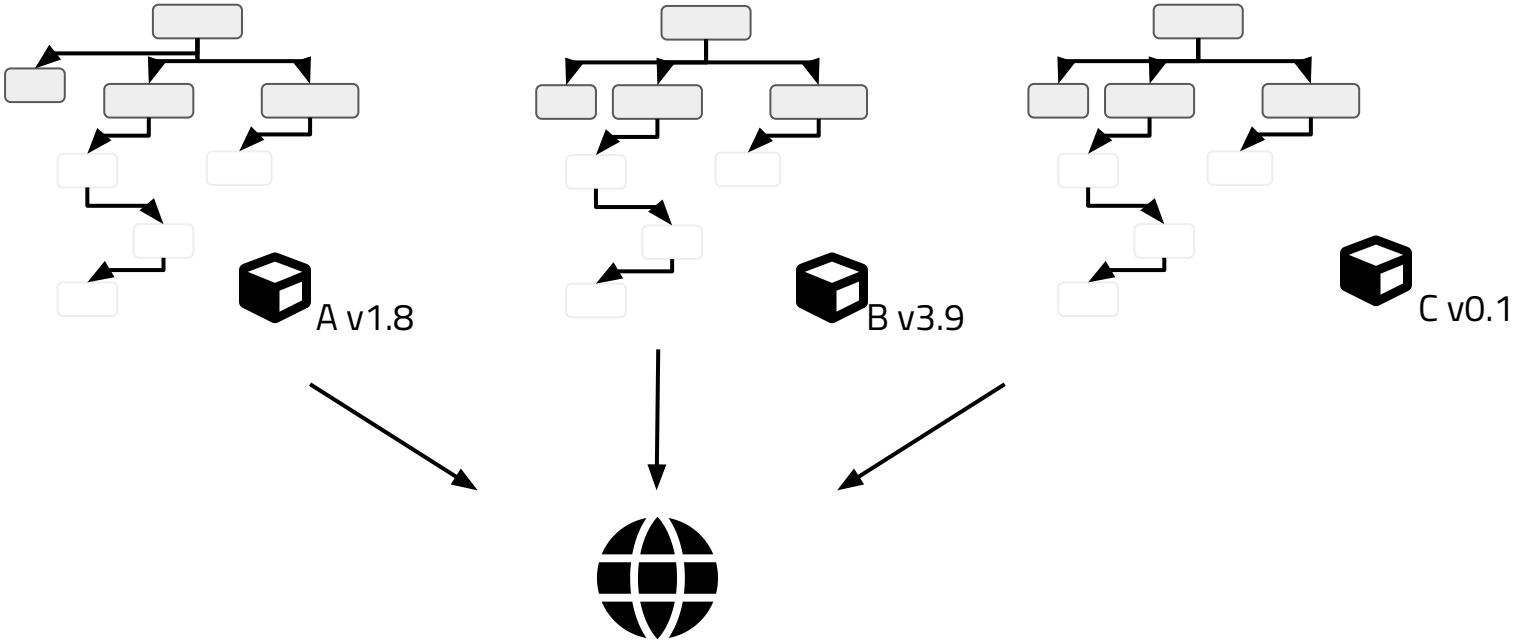
1.1.3

1.0.6

2.0.5



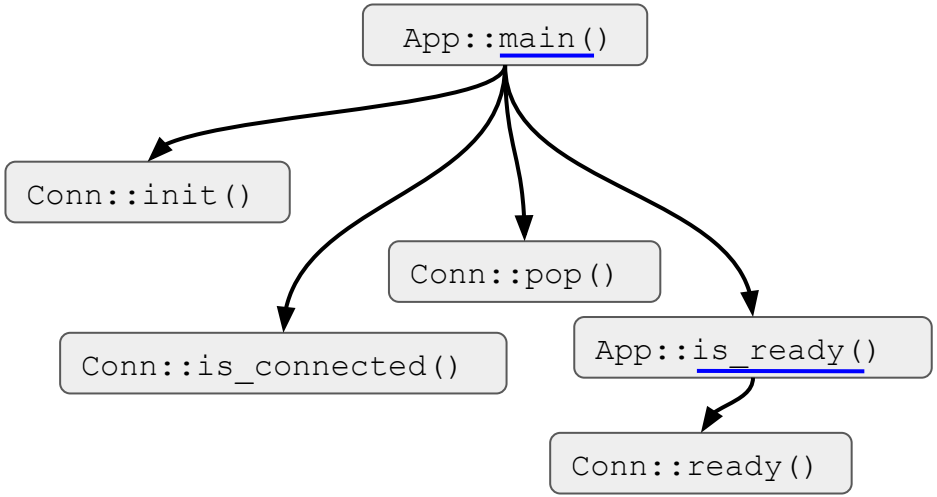
Dependency Network



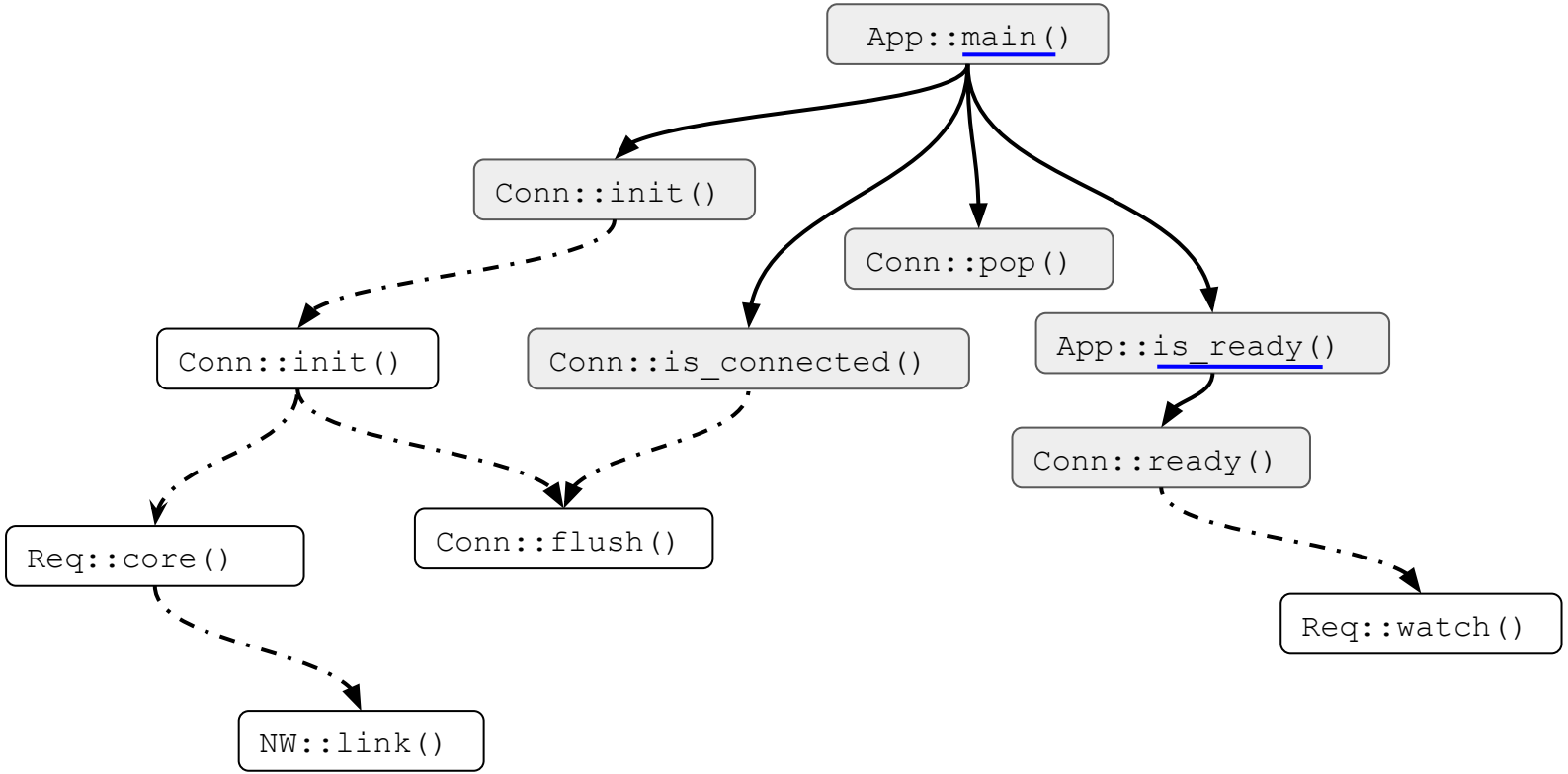
Resolving & merging all package dependency trees into one single network

Call graphs

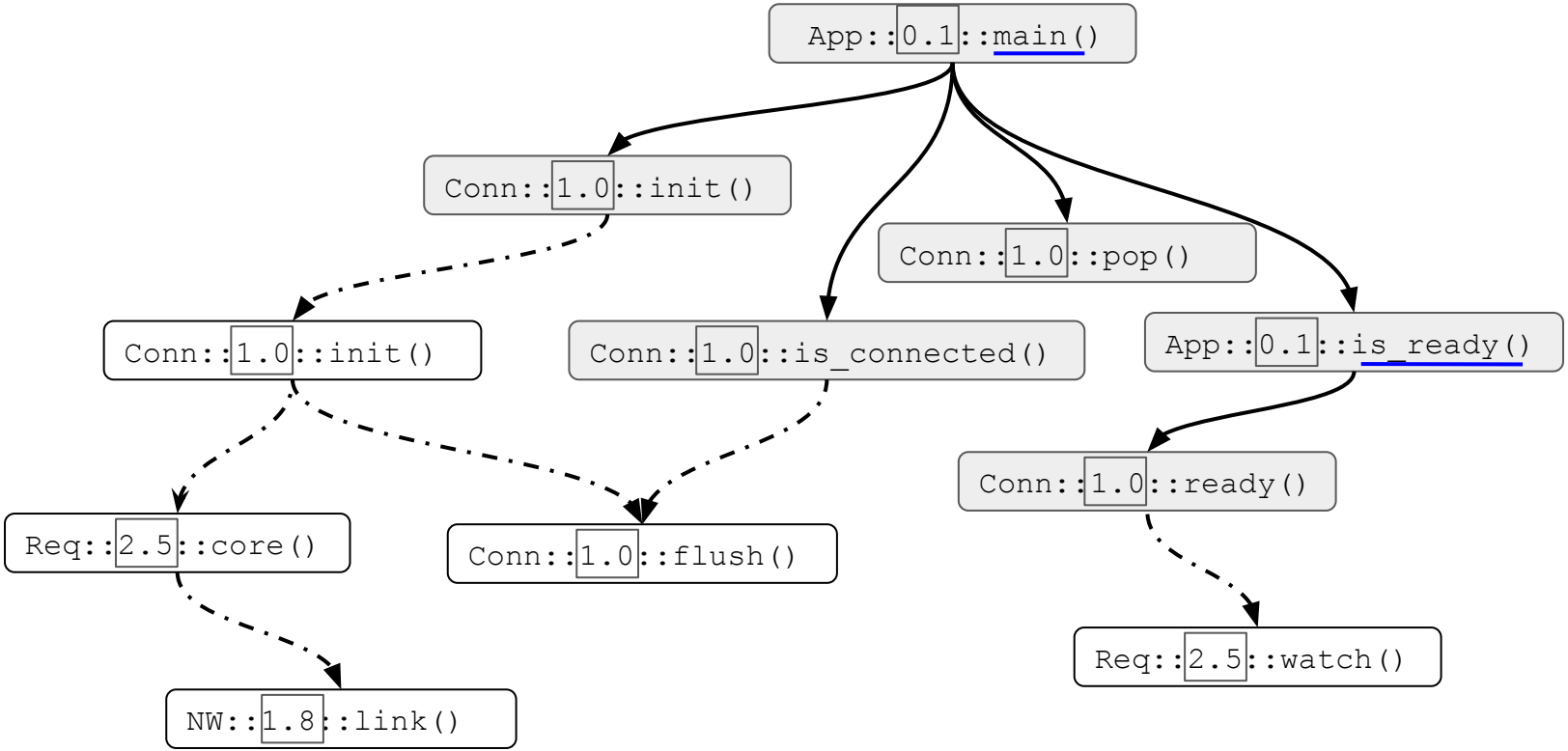
```
1  extern crate accepts;
2  extern crate send;
3
4  use accepts::Conn;
5  let is_ready = |conn: _| conn.ready();
6  fn main () {
7   let pipe = Conn::init();
8   let mut notifications = Vec::new();
9   while !is_ready(pipe);
10  // setup stuff
11  while pipe.is_connected() {
12   notifications.push(pipe.pop());
13  }
14 }
```



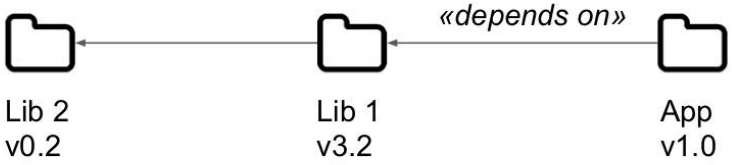
Our idea in a nutshell: go beyond a single program

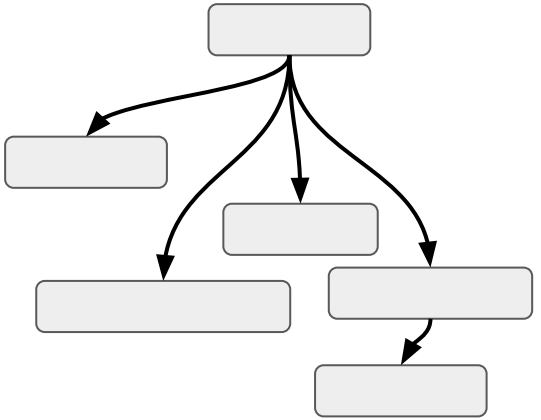


Our idea in a nutshell: go beyond a single program

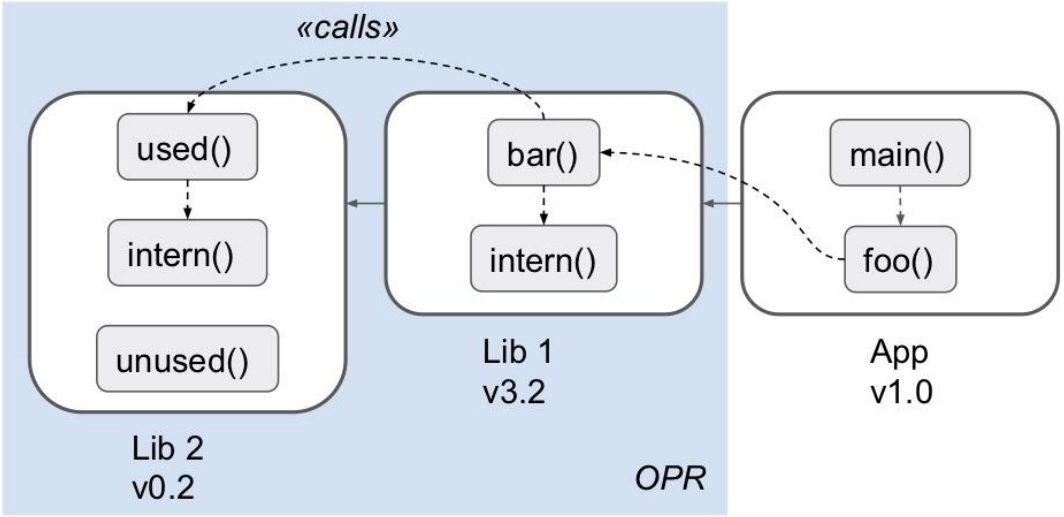


We merge two concepts into one





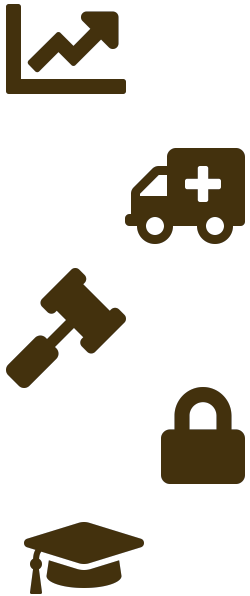
We merge two concepts into one

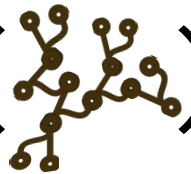


Call-based dependency networks (CDN)

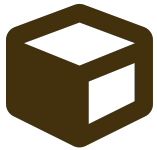
Data-driven insights for the community

```
cargo install praezi
cargo publish

 praezi run pre-publish ...failed!
    The removal of deprecated:
     -  def parse_old(txt: &str)
    will lead to 15% of crates.io
    to update once released.
    Permitted threshold: 2%.

 praezi analyze crate-adoption
     -  0.5.0   35%    -5%
     -  0.8.1   20%    +12%
```



.flatMap()?

Not a simple task...



Compile 22,352

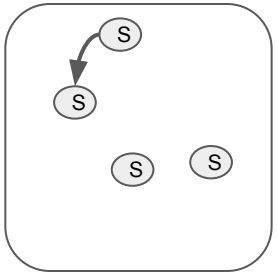
Entry Points?

Target architectures?

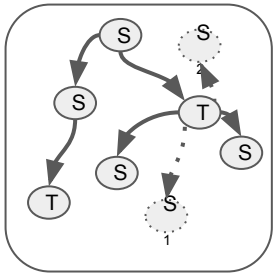
External Dependencies?

Version resolution? ~2.0.3

Precision?

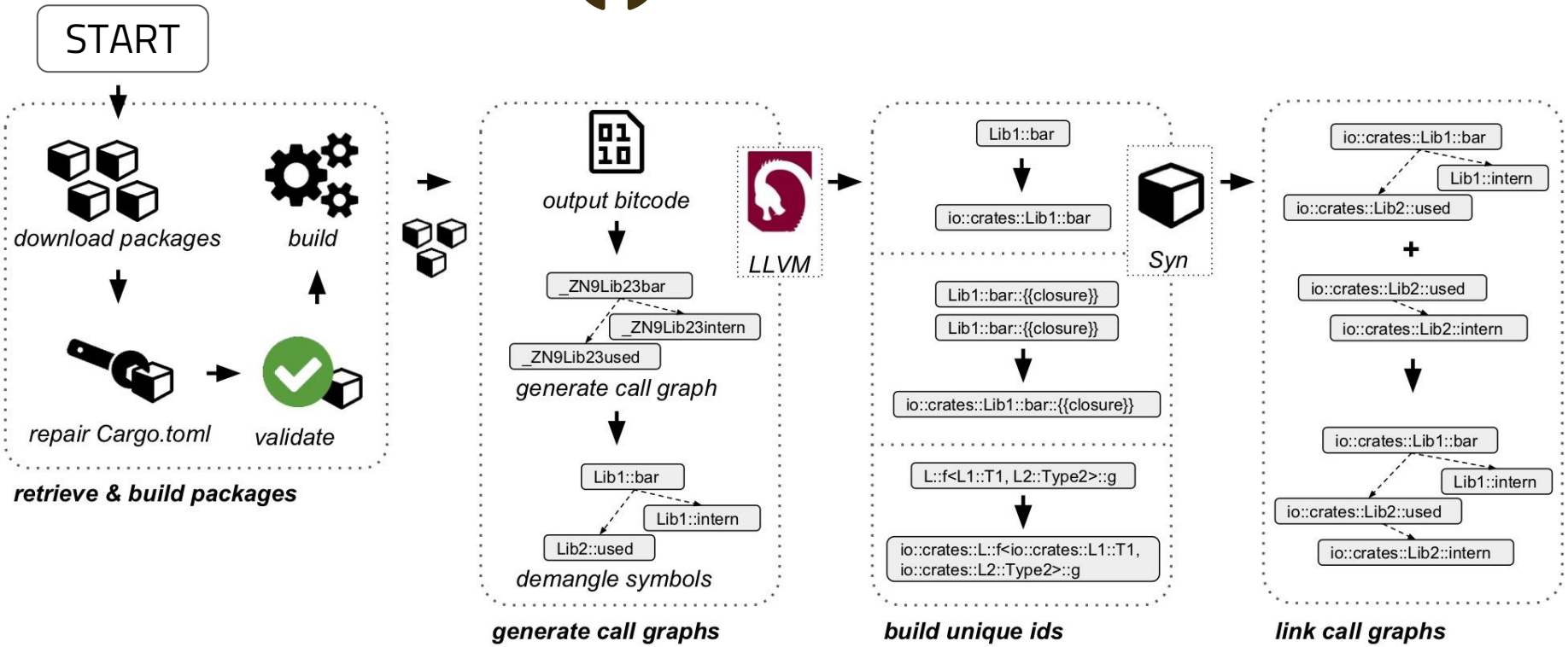


vs

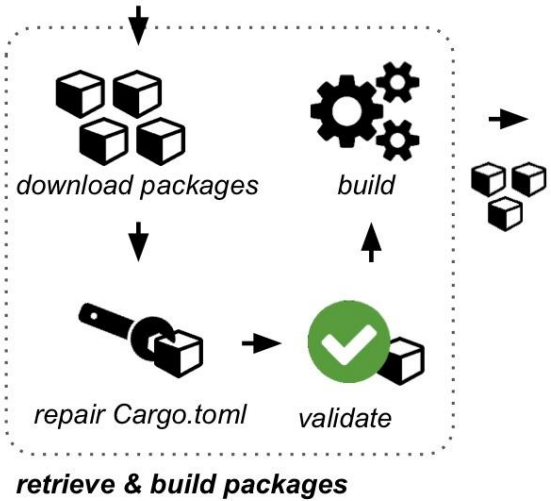


Soundness?

praezi/rust


START
download packages
build
repair Cargo.toml
validate
retrieve & build packages
output bitcode
_ZN9Lib23bar
_ZN9Lib23intern
_ZN9Lib23used
generate call graph
Lib1::bar
Lib1::intern
Lib2::used
demangle symbols
LLVM
generate call graphs
Lib1::bar
io::crates::Lib1::bar
Lib1::bar::{{closure}}
Lib1::bar::{{closure}}
io::crates::Lib1::bar::{{closure}}
L::f<L1::T1, L2::Type2>::g
io::crates::L::f<io::crates::L1::T1,
io::crates::L2::Type2>::g
Syn
build unique ids
io::crates::Lib1::bar
Lib1::intern
io::crates::Lib2::used
io::crates::Lib2::used
io::crates::Lib2::intern
io::crates::Lib1::bar
Lib1::intern
io::crates::Lib2::used
io::crates::Lib2::intern
link call graphs

Compiling



13,991 Packages

79,724 Releases

16th February 2018

Compiling 

```
Feb 25 20:22:31.744 ERRO (17944,allegro_dialog,0.0.11,stderr): error:  failed to load source for a dependency on `allegro`
```

```
error: Package `yup-oauth2 v1.0.6` does not have these features:  `nightly, with-serde-codegen`
```

```
error: failed to run custom build command
for `unwind-sys v0.1.1`
```

Compiling

Failure reason	**#Builds**
Compile error w. error code	13,509 (58%)
Compile error wo. error code, of which	7,272 (31%)
… code parsing errors	1,486
… conditional compilation errors	1,058
… dependency resolution errors	719
… type checking errors	278
… other errors	3,711
Custom build script failure	2,127 (9%)
Missing system dependencies	137 (< 1%)
Miscellaneous errors	18 (< 1%)
Σ	23,063

Compilation statistics

12,307 Packages

72,947 Releases

remove invalid manifests

10,831 Packages

49,844 Releases

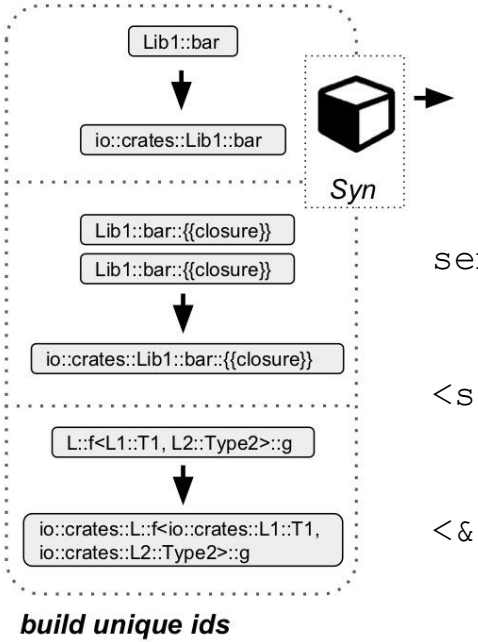
call graphs

69

hours

70%

Rustc symbols



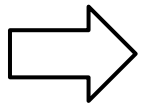

```
semver::ver::VersionReq::parse_deprecated

<semver::ver::VersionReq as core::cmp::PartialOrd>::le

<&'a T as core::fmt::Display>::fmt

core::fmt::num::<impl core::fmt::Display for u64>::fmt
```

jhejderup/syn

```
semver::ver::VersionReq::parse_deprecated

<semver::ver::VersionReq as core::cmp::PartialOrd>::le

<&'a T as core::fmt::Display>::fmt

core::fmt::num::<impl core::fmt::Display for u64>::fmt
```

Universal Function Identifier

```
[package]
name = "cool"
version = "0.1.0"
authors = ["Joseph Hejderup <joseph.hejderup@gmail.com>"]

[dependencies]
git2 = "*"
regex = "0.2.x"
cargo = "^1.2"
```



Cargo.lock

```
git2 = “1.2.0”
regex = “0.2.0”
cargo = “1.2.9”
```

package name and version

```
io::crates::git2::v_1_2_0::git::core::pull
```

ecosystem

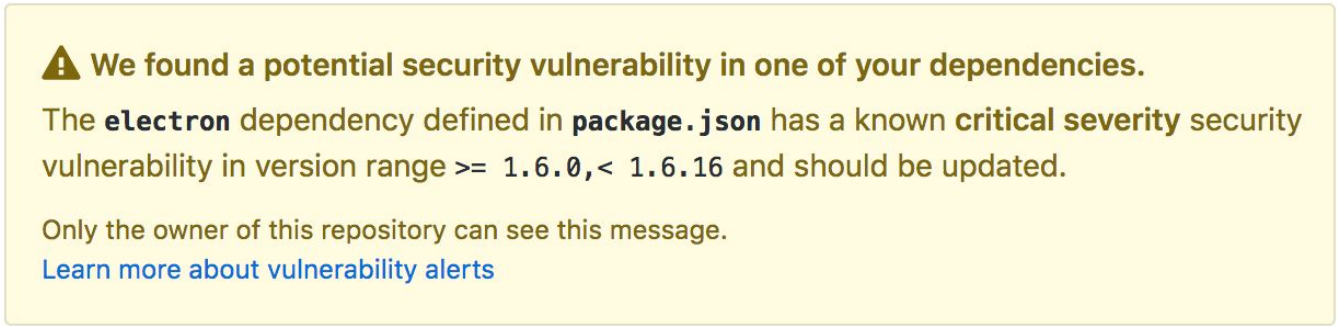
lib

module

fn

Query time (no live demo, too shy :/)

Checking for known vulnerabilities



Checking for known vulnerabilities

6

advisories

13 functions

dependency network (PDN)

8,106 Packages

RustPräzi (CDN)

649 Packages

Affected packages

482

Baseline (direct dependencies only)

PDN: 0.30

CDN: 0.87

RustSec now add functions in advisories!

tarcieri commented on Nov 28, 2018 — Member

RustPräzi is a crater-like tool which builds a call graph across all of the crates published to crates.io:

https://internals.rust-lang.org/t/prototype-dev-tool-rustprazi-a-tool-to-build-an-entire-call-graph-of-crates-io/8912

It would be interesting to use this tool, perhaps in conjunction with crates-audit, to generate a list of impacted crates based on this call graph.

Add new affected functions attribute to template #82

Merged **tarcieri** merged 1 commit into `RustSec:master` from `praezi:master` 24 days ago

Conversation 2 · Commits 1 · Checks 0 · Files changed 1

Inventitech commented 25 days ago — Contributor

Refs #68

Small deprecation study

How many would be affected by removal of deprecated functions?

`#[Deprecation]`

Find functions annotated for deprecation

11 functions from

6 Package releases

Findings

311

How many dependents?

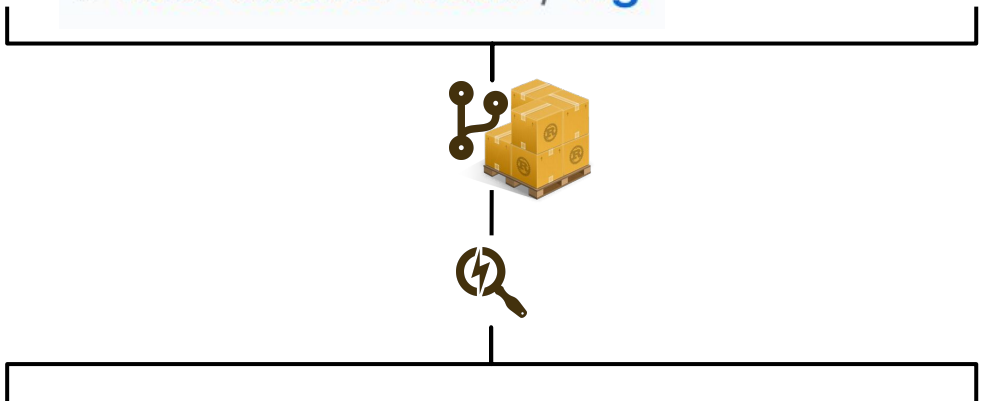
52%

Potentially both directly or indirectly affected by deprecation

RustPräzi  Community

Community-driven analyses

rust-lang-nursery / **crater**
rust-lang-nursery / **ecosystem-wg**
rust-secure-code / **wg**



Which crates call a vulnerable function?
How many unsafe code blocks are called?
Which deprecated functions are central to crates.io?

A step towards it...

www.dep.management