Usable Language-Based Verification

Niki Vazou
IMDEA

Software Bugs are Everywhere

Airbus A400M crashed due to a software bug.
— May 2015

Software Bugs are Everywhere

The Heartbleed Bug.
Buffer overread in OpenSSL. 2015

Verification Prevents Bugs!

Verification Prevents Bugs!

Project Everest.
Builds a Verified HTTPS Stack.

Inria

Microsoft Research

Carnegie Mellon University

Verification Prevents Bugs!

Prove end-to-end Correctness of Whole Systems

Princeton

Penn

Yale

MIT

But Requires Experts

Princeton Penn Yale MIT

My Goal:

Make Verification Accessible

My Approach:

Turn a Language into a Verifier

Haskell

General Purpose Programming Language

1 Python

...

25 Haskell

...

36 Erlang

...

45 OCaml

Popularity of Programming Languages
by spectrum.ieee

Haskell

+

Refinement Types

=

Haskell

```
take :: [a] -> Int -> [a]
```

```
> take [1,2,3] 2
> [1,2]
```

Haskell

```
take :: [a] -> Int -> [a]
```

```
> take [1,2,3] 500
> ???
```

Refinement Types

```
take :: xs:[a] -> {i:Int | i < len xs} -> [a]
```


```
take :: xs:[a] -> {i:Int | i < len xs} -> [a]
```

```
> take [1,2,3] 500
> Refinement Type Error!
```

LiquidHaskell

Use Haskell's syntax, runtime, and **users**!

Used in **Industry**: to speed up code

AWAKE Well-Typed

Used in **Education**: in Haskell courses!

UNIVERSITY OF MARYLAND 18 56

COLLEGE BRYN MAWR SIGILL VERITATEM DILEXI

UNIVERSITY OF CALIFORNIA SAN DIEGO LET THERE BE LIGHT

I. Static Checks: Fast & Safe Code

II. Application: Speed up Parsing

III. Status: Industry & Education

I. Static Checks: Fast & Safe Code

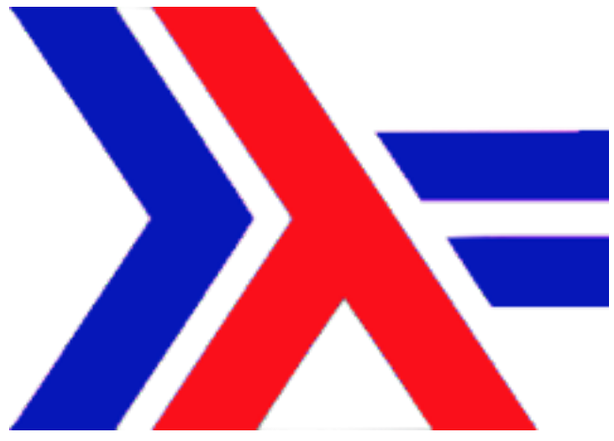
In theory Haskell is already SAFE!

Haskell

Functional Programing Language

Safe because of

Strong Typing + λ-calculus



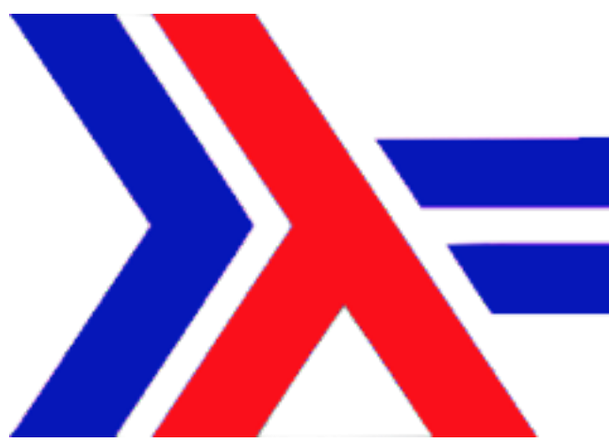
Haskell

Practical Programing Language

Fast Memory Manipulation

with C wrappers

Allowing overread bugs

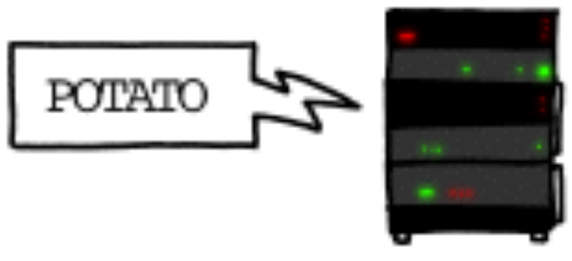


The Heartbleed Bug

Buffer overread in OpenSSL. 2015

HOW THE HEARTBLEED BUG WORKS:

SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).



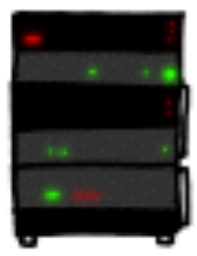
SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).

User Olivia from London wants pages about "man bees in car why". Note: Files for IP 375.381. 283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2cab9ff89bd3bff8

HMM...

User Olivia from London wants pages about "man bees in car why". Note: Files for IP 375.381. 283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2cab9ff89bd3bff8

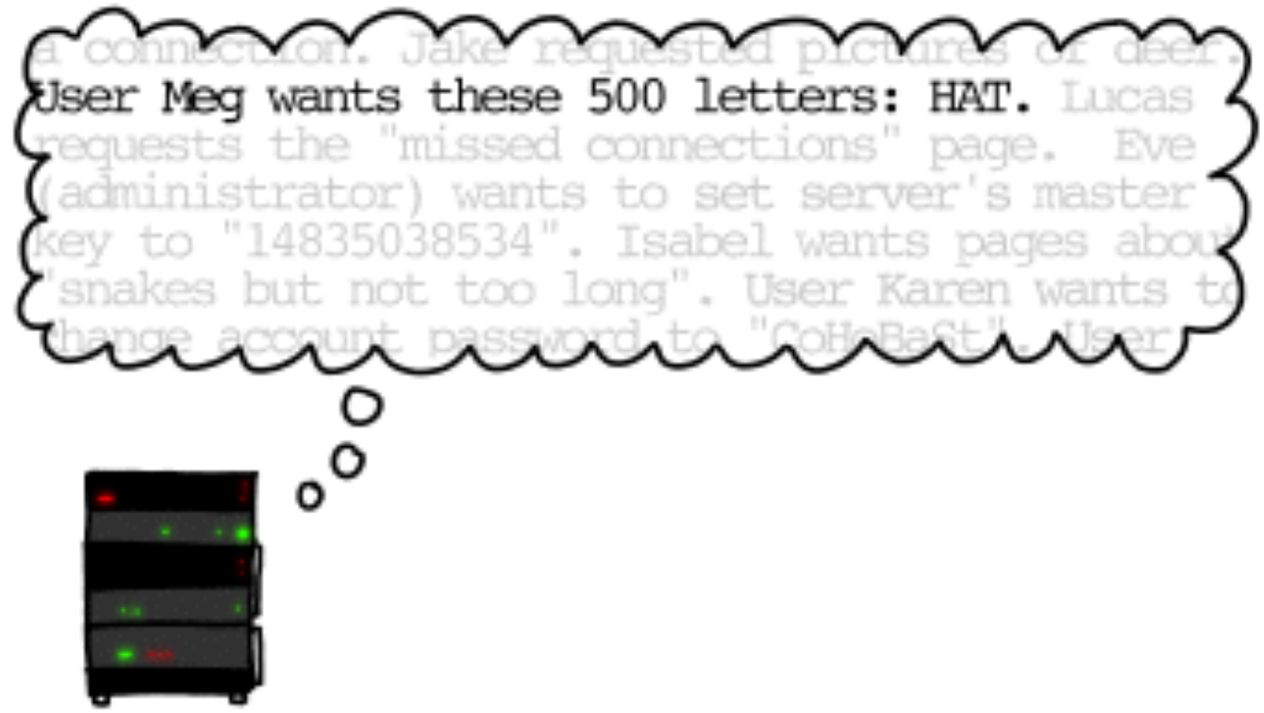
BIRD

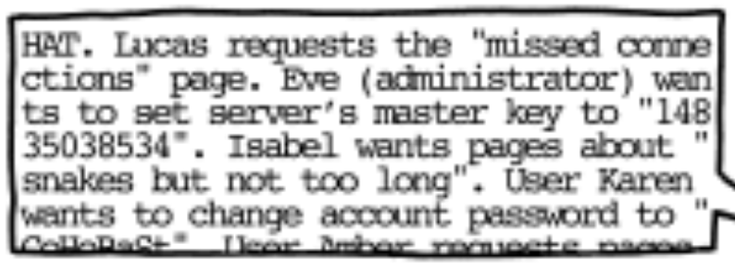


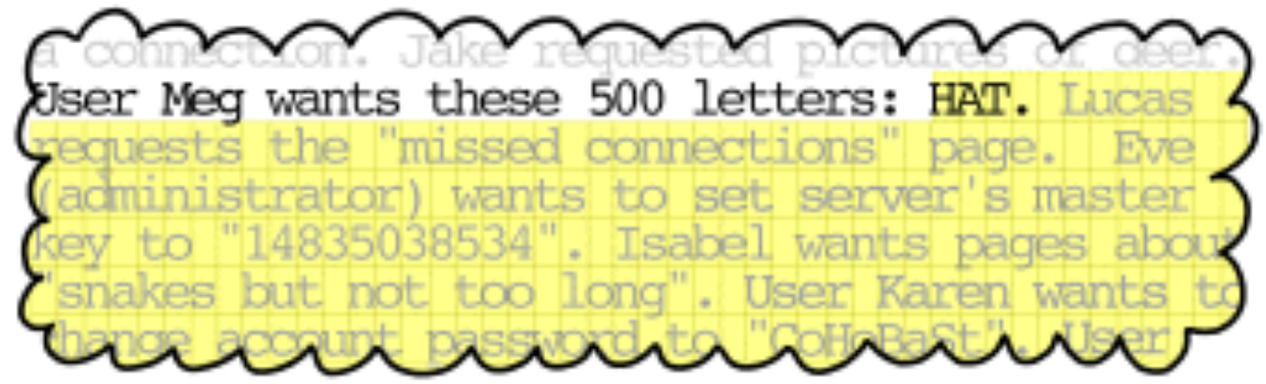
SERVER, ARE YOU STILL THERE?

User Meg wants these 500 letters: HAT. Lucas

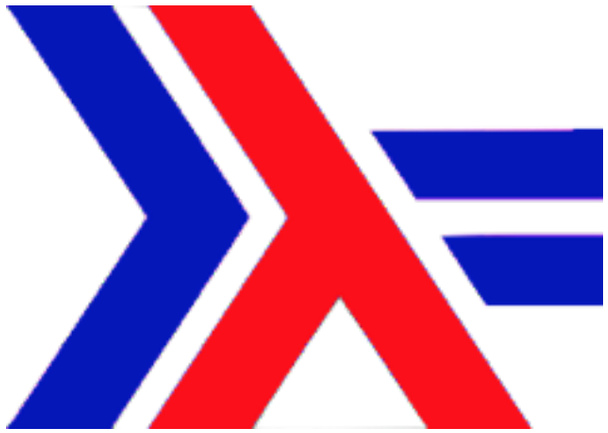
SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).







in



```
module Data.Text where
take :: t:Text -> i:Int -> Text
```

```
> take "hat" 500
> *** Exception: Out Of Bounds!
```

Runtime Checks

```
take :: t:Text -> i:Int -> Text
take t i | i < len t
  = Unsafe.take t i
take t i
  = error "Out Of Bounds!"
```

Safe, but slow!

No Checks

```
take :: t:Text -> i:Int -> Text
take t i | i < len t
  = Unsafe.take t i
take t i
  = error "Out Of Bounds!"
```

Fast, but unsafe!

No Checks

```
take :: t:Text -> i:Int -> Text
take t i | i < len t
  = Unsafe.take t i
take t i
  = error “Out Of Bounds!”
```

```
> take "hat" 500
> “hat\58456\2594\SOH\NUL…
```

Overread

Static Checks

```
take :: t:Text -> i:Int -> Text
take t i | i < len t
  = Unsafe.take t i
take t i
  = error “Out Of Bounds!”
```

Static Checks

```
take :: t:Text -> i:{i < len t} -> Text
take t i | i < len t
  = Unsafe.take t i
take t i
  = error "Out Of Bounds!"
```

Static Checks

```
take :: t:Text -> i:{i < len t} -> Text
take t i | i < len t
  = Unsafe.take t i
take t i
  = error "Out Of Bounds!"
```

Static Checks

```
take :: t:Text->i:{i < len t}->Text
take t i
 = Unsafe.take t i
```

Static Checks

```
take :: t:Text->i:{i < len t}->Text
take t i
 = Unsafe.take t i
```

```
> take "hat" 500
```

Type Error

Refinement Types

Checks valid arguments, under facts.

Checks valid arguments, under facts.

```
take :: t:Text->{v|v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in take x 500
```

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text
heartbleed = let x = "hat"
             in  take x 500
```

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

SMT-query

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v|v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

SMT-invalid

`len x = 3 => v = 500 => v < len x`

Checks valid arguments, under facts.

```
take :: t:Text->{v|v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

Checker reports **Error**

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

Checker reports **Error**

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in  take x 2
```

Checker reports **OK**

SMT-valid

```
len x = 3 => v = 2 => v < len x
```

Checks valid arguments, under facts.

Refinement Types for Haskell, ICFP'14

by **Vazou**, Seidel, Jhala, Vytiniotis, and Peyton-Jones

Checks valid arguments, under facts.

Static Checks

I. Static Checks: Fast & Safe Code

II. Application: Speed up Parsing

III. Status: Industry & Education

I. Static Checks: Fast & Safe Code

II. Application: Speed up Parsing

III. Status: Industry & Education

II. Application: Speed up Parsing

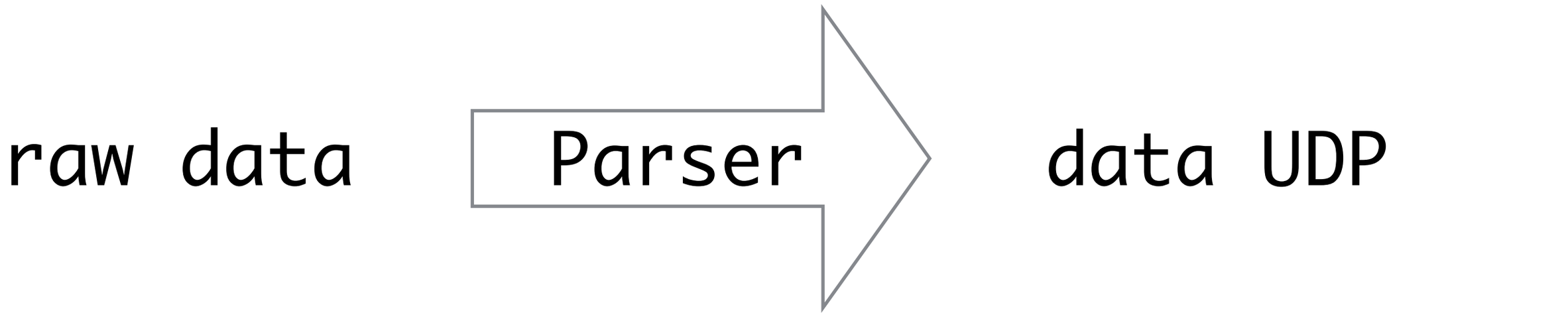
Application: Speed up Parsing

Simplified Application of Liquid Haskell

by Gabriel Gonzalez

Application: Speed up Parsing

UDP: User Datagram Protocol



Application: Speed up Parsing

```
data UDP = UDP
    { udpSrcePort :: Text   -- 2 chars
    , udpDestPort :: Text   -- 2 chars
    , udpLength   :: Text   -- 2 chars
    , udpChecksum :: Text   -- 2 chars
    }
```

Application: Speed up Parsing

```
udpP :: Text -> UDP
udpP bs =
  let (udp1, bs1) = splitAt 2 bs
  let (udp2, bs2) = splitAt 2 bs1
  let (udp3, bs3) = splitAt 2 bs2
  let (udp4, bs4) = splitAt 2 bs3
  in UDP (udp1 upd2 udp3 upd4)
```

Safe but Slow (4 runtime checks)

Solution: Merge checks

Application: Speed up Parsing

```haskell
udpP :: Text -> Maybe UDP
udpP bs =
  if length bs >= 8 then
    let (udp1, bs1) = US.splitAt 2 bs
    let (udp2, bs2) = US.splitAt 2 bs1
    let (udp3, bs3) = US.splitAt 2 bs2
    let (udp4, bs4) = US.splitAt 2 bs3
    in Just (UDP udp1 upd2 udp3 upd4)
  else Nothing
```

Safe and Fast (1 runtime check!)

Application: Speed up Parsing

```
udpP :: Text -> Maybe UDP
udpP bs =
  if length bs >= 8 then
    let (udp1, bs1) = US.splitAt 2 bs
    let (udp2, bs2) = US.splitAt 2 bs1
    let (udp3, bs3) = US.splitAt 4 bs2
    let (udp4, bs4) = US.splitAt 2 bs3
    in Just (UDP udp1 upd2 udp3 upd4)
  else Nothing
```

Safe and Fast, bur error prone

Application: Speed up Parsing

```
udpP :: Text -> Maybe UDP
udpP bs =
  if length bs >= 8 then
    let (udp1, bs1) = US.splitAt 2 bs
```

```
splitAt :: i:Int -> t:{i < len t} ->
 (tl:{i = len tl}, tr:{len tr = len t - i})
```

```
    in Just (UDP udp1 upd2 udp3 upd4)
  else Nothing
```

Enforce Static Checks!

Application: Speed up Par

GHC OK, but Liquid Error

Error

```
udpP :: Text -> Maybe UDP
udpP bs =
  if length bs >= 8 then
    let (udp1, bs1) = US.splitAt 2 bs
    let (udp2, bs2) = US.splitAt 2 bs1
    let (udp3, bs3) = US.splitAt 4 bs2
    let (udp4, bs4) = US.splitAt 2 bs3
    in Just (UDP udp1 upd2 udp3 upd4)
  else Nothing
```

Enforce Static Checks!

Application: Speed up Parsing

OK

```
udpP :: Text -> Maybe UDP
udpP bs =
  if length bs >= 8 then
    let (udp1, bs1) = US.splitAt 2 bs
    let (udp2, bs2) = US.splitAt 2 bs1
    let (udp3, bs3) = US.splitAt 2 bs2
    let (udp4, bs4) = US.splitAt 2 bs3
    in Just (UDP udp1 upd2 udp3 upd4)
  else Nothing
```

Provably Correct & Faster (x6) Code!

Application: Speed up Parsing

```
udpP :: Text -> Maybe UDP
udpP bs =
  if length bs >= 8 then
    let (udp1, bs1) = US.splitAt 2 bs
    let (udp2, bs2) = US.splitAt 2 bs1
    let (udp3, bs3) = US.splitAt 2 bs2
    let (udp4, bs4) = US.splitAt 2 bs3
    in Just (UDP udp1 upd2 udp3 upd4)
  else Nothing
```

Provably Correct & Faster (x6) Code!

Haskell Code: SMT-Automatic Verification

Application: Speed up Parsing

Provably Correct & Faster (x6) Code!

SMT-Automatic Verification

SMT-Automatic Verification

How expressive can we get?

SMT-Verification

Critical Properties, GOAL

"The plane will not crash!"

Expressiveness

Refinement Types for Haskell, ICFP'14

"Your passwords are safe!"

Expressiveness

SMT-Verification

Critical Properties, GOAL

"The plane will not crash!"

Theorem Proving, POPL'18

"If f(x) < f(x+1), then f is monotonic"

Refinement Types for Haskell, ICFP'14

"Your passwords are safe!"

SMT-Verification

Theorem Proving, POPL'18

"If f(x) < f(x+1), then f is monotonic"

Expressiveness

Refinement Types for Haskell, ICFP'14

"Your passwords are safe!"

Liquid Haskell on papers

Expressiveness

Refinement Reflection, POPL'18

by **Vazou**, Tondwalkar, Choudhury, Scott, Newton, Wadler, and Jhala

Refinement Types for Haskell, ICFP'14

by **Vazou**, Seidel, Jhala, Vytiniotis, and Peyton-Jones

Liquid Haskell on papers

Expressiveness

Refinement Reflection, POPL'18
by **Vazou**, Tondwalkar, Choudhury, Scott, Newton, Wadler, and Jhala

Bounded Refinement Types, ICFP'15
by **Vazou**, Bakst, and Jhala

Abstract Refinement Types, ESOP'13
by **Vazou**, Rondon, and Jhala

Refinement Types for Haskell, ICFP'14
by **Vazou**, Seidel, Jhala, Vytiniotis, and Peyton-Jones

Liquid Haskell on github

ucsd-progsys / liquidhaskell

Unwatch 22 | Star 473 | Fork 75

Code | Issues 201 | Pull requests 5 | Projects 0 | Wiki | Insights | Settings

Liquid Types For Haskell

Edit

Add topics

8,382 commits | 94 branches | 19 releases | 38 contributors

Branch: develop | New pull request | Create new file | Upload files | Find file | Clone or download

nikivazou Merge pull request #1223 from ucsd-progsys/HaskellFunInRefs ... Latest commit 82f5baa 5 days ago

benchmarks	move tests into pos	a month ago
devel	Fix travis error	6 days ago

Liquid Haskell main dev team

Niki Vazou & Ranjt Jhala,
Liquid Haskell dev team

Liquid Haskell in the real world

Education

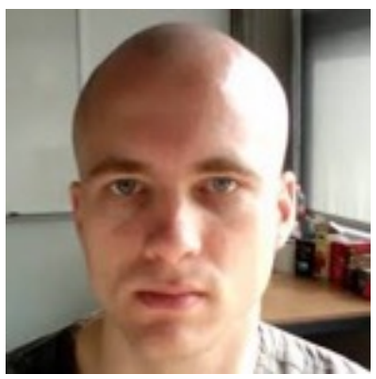
Will Kunkel,
undergrad @UMD

Niki Vazou & Ranjt Jhala,
Liquid Haskell dev team

Rachel Xu & Xinyue Zhang,
undergrads @Bryn Mawr College

Industry

Gabriel Gonzalez
Awake Security



Edsko de Vries
Well-Typed

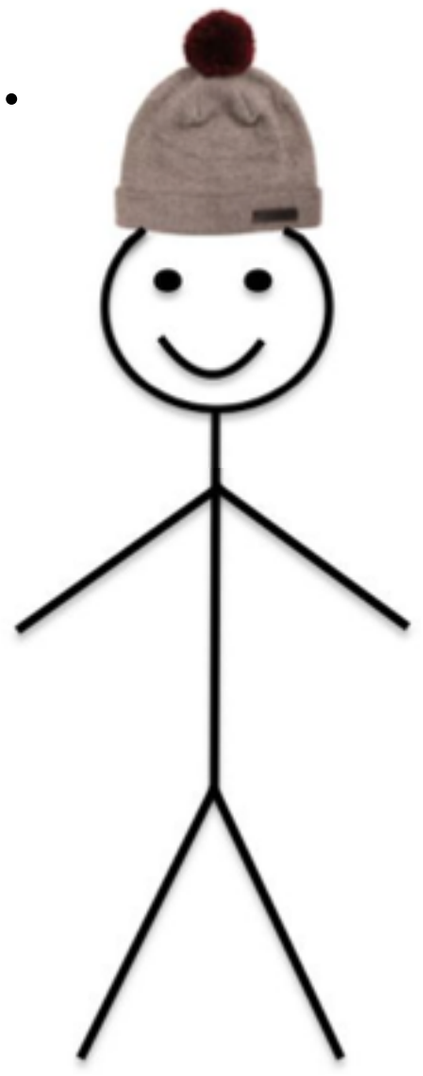
Liquid Haskell in Education

This is Will Kunkel.

Will took my undergrad course on Haskell.

Will learnt Liquid Haskell in 2 weeks.

Will was **3rd** in POPL'18 **Student Research Competition** with his project "Comparing Liquid Haskell and Coq"



Will is smart.

Be like Will.

Liquid Haskell in Education

Two winners in POPL'18 Student Research Competition

"Comparing Liquid Haskell and Coq"

Will Kunkel,
undergrad @UMD

"Comparing Dependent Haskell, Liquid Haskell and F*"

Rachel Xu & Xinyue Zhang,
undergrads @Bryn Mawr College

Liquid Haskell in Education

Two winners in POPL'18 Student Research Competition

"Comparing Liquid Haskell and Coq"

Will Kunkel,
undergrad @UMD

"Comparing Dependent Haskell, Liquid Haskell and F*"

Rachel Xu & Xinyue Zhang,
undergrads @Bryn Mawr College

Liquid Haskell in the real world

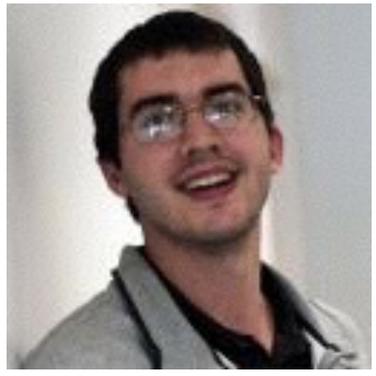
Education

Will Kunkel,
undergrad @UMD

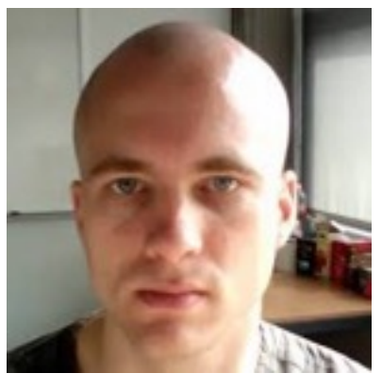
Rachel Xu & Xinyue Zhang,
undergrads @Bryn Mawr College

Niki Vazou & Ranjt Jhala,
Liquid Haskell dev team

Industry



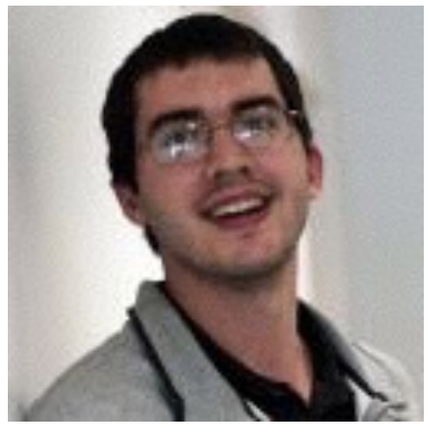
Gabriel Gonzalez
Awake Security



Edsko de Vries
Well-Typed

Liquid Haskell in Industry

Gabriel Gonzalez



AWAKE

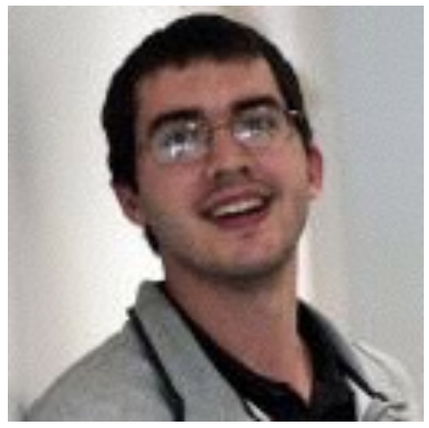
Static checks during parsing.

Provably Correct & Faster (x6) Code!

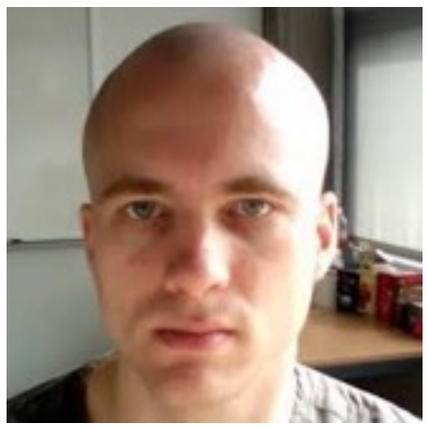
Huge speedup for internet traffic parsing.

Liquid Haskell in Industry

Gabriel Gonzalez

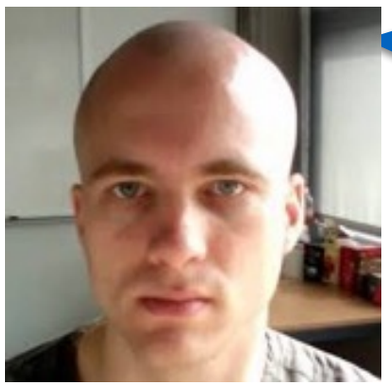


AWAKE

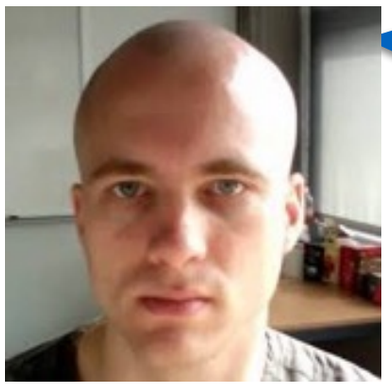


Well-Typed

Edsko de Vries

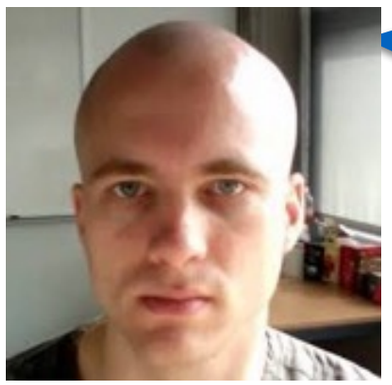


I am a Haskell consultant at a **cryptocurrency/blockchain** company.
We have a blockchain algorithm written **in paper** & a **Haskell implementation**.
We want Liquid Haskell to connect them.



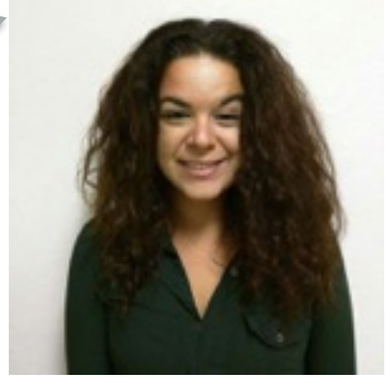
I am a Haskell consultant at a **cryptocurrency/blockchain** company. We have a blockchain algorithm written **in paper** & a **Haskell implementation**. We want Liquid Haskell to connect them.

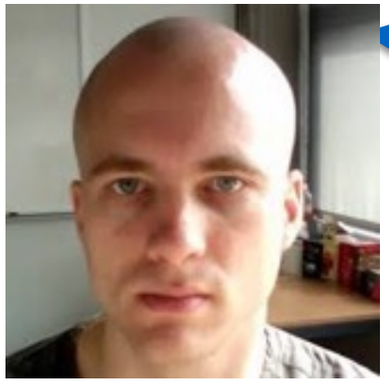
Awesome! Lmk if you need anything!



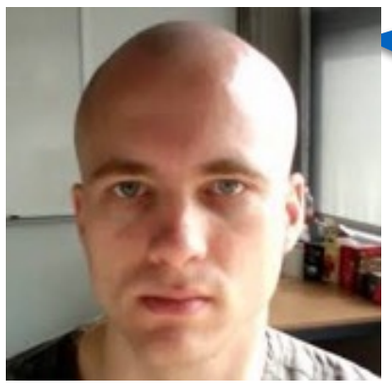
I am a Haskell consultant at a **cryptocurrency/blockchain** company. We have a blockchain algorithm written **in paper** & a **Haskell implementation**. We want Liquid Haskell to connect them.

Awesome! Lmk if you need anything!



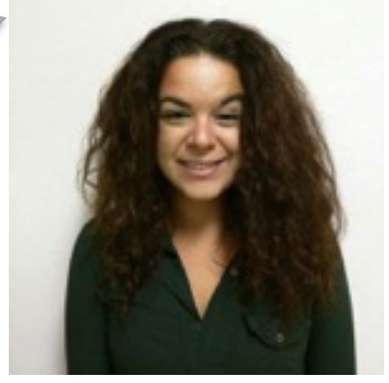


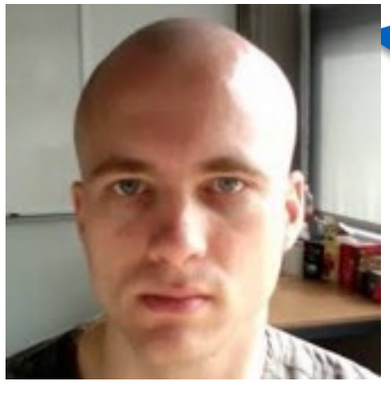
I want **interactive proof generation**!



I am a Haskell consultant at a **cryptocurrency/blockchain** company. We have a blockchain algorithm written **in paper** & a **Haskell implementation**. We want Liquid Haskell to connect them.

Awesome! Lmk if you need anything!



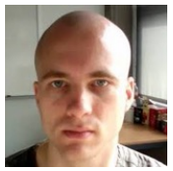


I want **interactive proof generation**!

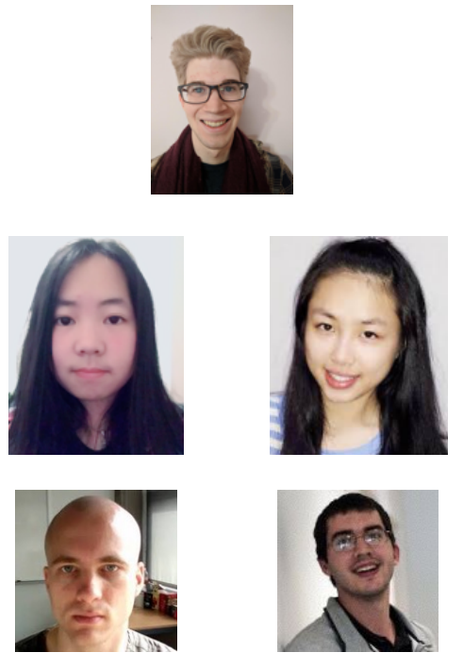
Liquid Haskell has many users

7,765 downloads

many users, but two main devs



many users, but two main devs



Goal: Expand the Liquid Haskell Team

Goal: Expand the Liquid Haskell Team

To formalize & implement research ideas

e.g.,

compiler optimizations,
proof assistance,
real system verification.

Vision:
Embed Verification in Haskell Programming

Vision:
Embed Verification in Haskell Programming

Specs are just comments **inside** the languages, ...
thus, learning effort is small.

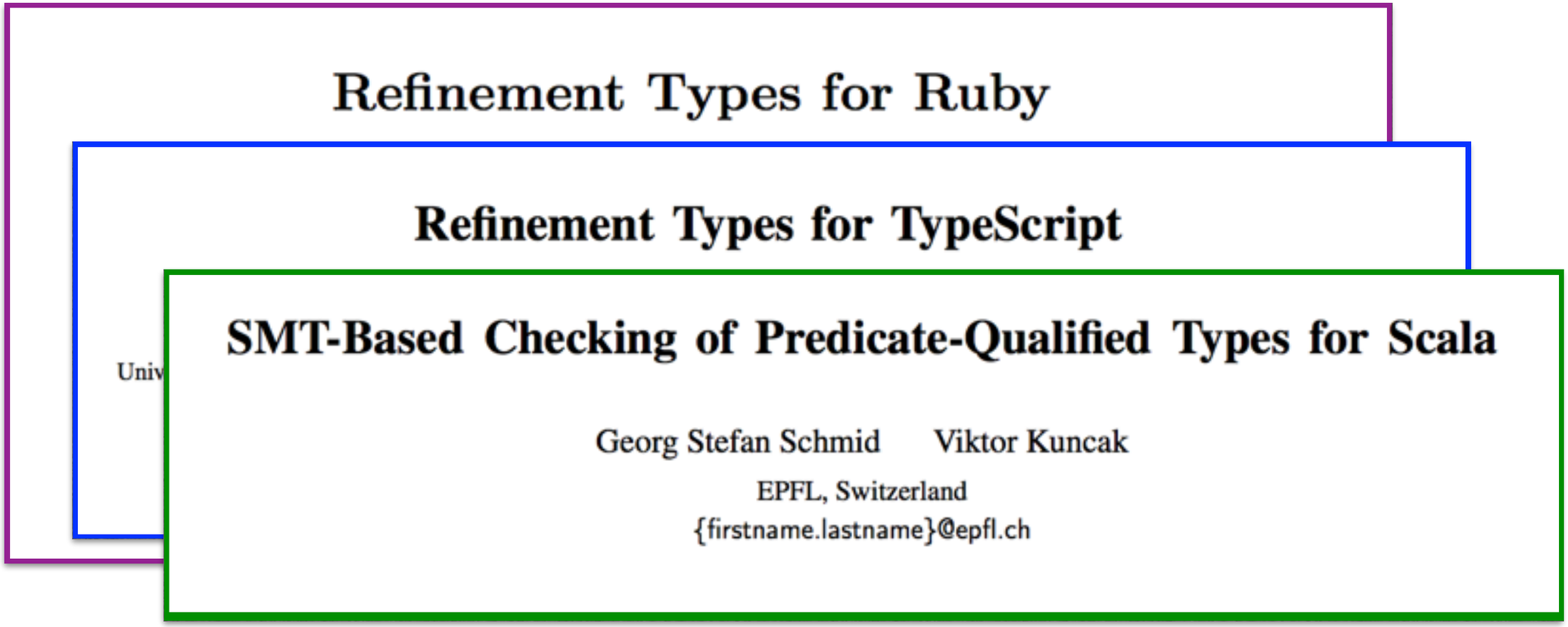
Semi-**automatically** machine checked, via SMTs.

For runtime **optimizations**, by the user or the compiler.

Vision:
Embed Verification in ~~Haskell~~ Programming

mainstream

Ruby, **JavaScript**, **Scala**, ...



Embed Verification in Haskell Programming

I. Static Checks: Fast & Safe Code

II. Application: Speed up Parsing

III. Status: Industry & Education

Thanks!