You Can't Touch This

WG2.8 meeting 2012

Albert-Ludwigs-Universität Freiburg

Peter Thiemann Manuel Geffken Phillip Heidegger

University of Freiburg

thiemann@informatik.uni-freiburg.de

07 November 2012

Motivation

92%

of all websites use

JavaScript

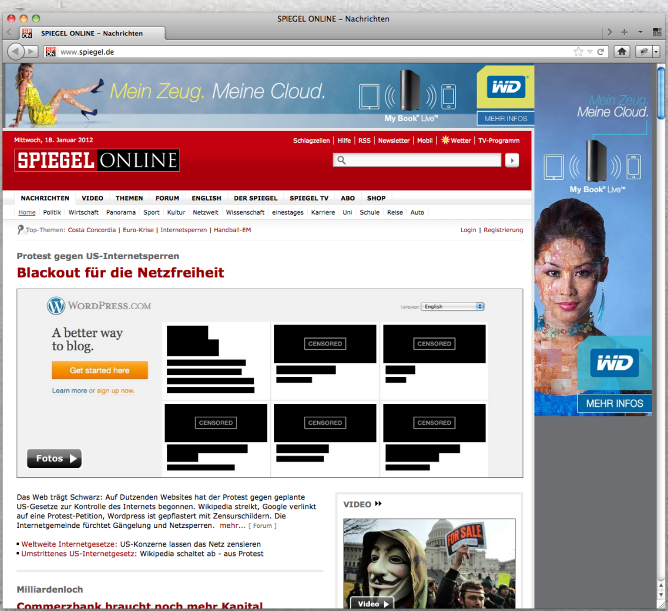
according to: `http://w3techs.com/`, 30/09/12

Thesis

The Full Employment Theorem for Research on JavaScript

- There will always be another JavaScript feature

Situation of a Web Programmer



SPIEGEL ONLINE – Nachrichten

www.spiegel.de

Mittwoch, 18. Januar 2012

Schlagzeilen | Hilfe | RSS | Newsletter | Mobil | Wetter | TV-Programm

SPIEGEL ONLINE

NACHRICHTEN VIDEO THEMEN FORUM ENGLISH DER SPIEGEL SPIEGEL TV ABO SHOP

Home Politik Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft einestages Karriere Uni Schule Reise Auto

Top-Themen: Costa Concordia | Euro-Krise | Internetsperren | Handball-EM

Login | Registrierung

Protest gegen US-Internetsperren

Blackout für die Netzfreiheit

WordPress.com

Language English

A better way to blog.

Get started here

Learn more or sign up now.

CENSORED CENSORED CENSORED CENSORED CENSORED

Fotos

Das Web trägt Schwarz: Auf Dutzenden Websites hat der Protest gegen geplante US-Gesetze zur Kontrolle des Internets begonnen. Wikipedia streikt, Google verlinkt auf eine Protest-Petition, Wordpress ist gepflastert mit Zensurschildern. Die Internetgemeinde fürchtet Gängelung und Netzsperren. mehr... [Forum]

- Weltweite Internetgesetze: US-Konzerne lassen das Netz zensieren
- Umstrittenes US-Internetgesetz: Wikipedia schaltet ab - aus Protest

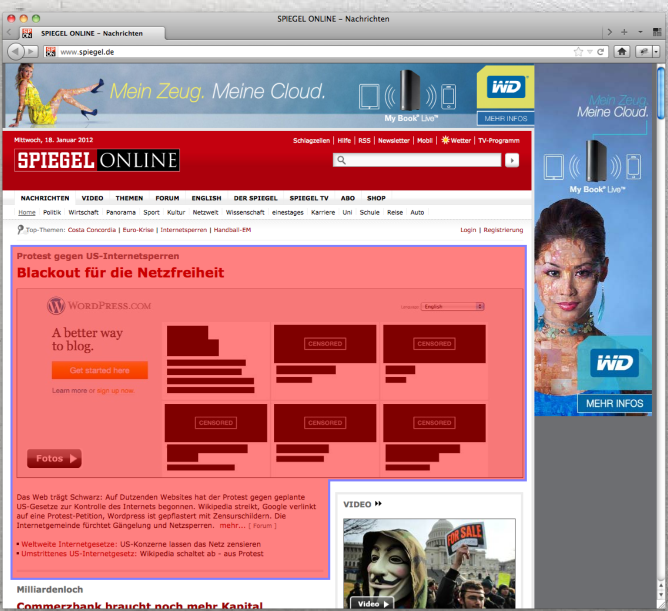
VIDEO

Video

Milliardenloch

Commerzbank braucht noch mehr Kapital

Situation of a Web Programmer


SPIEGEL ONLINE – Nachrichten
www.spiegel.de
Mein Zeug. Meine Cloud.
My Book Live
WD
MEHR INFOS
Mittwoch, 18. Januar 2012
Schlagzeilen | Hilfe | RSS | Newsletter | Mobil | Wetter | TV-Programm
SPIEGEL ONLINE
NACHRICHTEN VIDEO THEMEN FORUM ENGLISH DER SPIEGEL SPIEGEL TV ABO SHOP
Home Politik Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft einestages Karriere Uni Schule Reise Auto
Top-Themen: Costa Concordia | Euro-Krise | Internetsperren | Handball-EM
Login | Registrierung
WordPress.com
English
A better way to blog.
Get started here
Learn more or sign up now.
CENSORED
CENSORED
CENSORED
CENSORED
CENSORED
Fotos
VIDEO
FOR SALE
Video

Protest gegen US-Internetsperren

Blackout für die Netzfreiheit

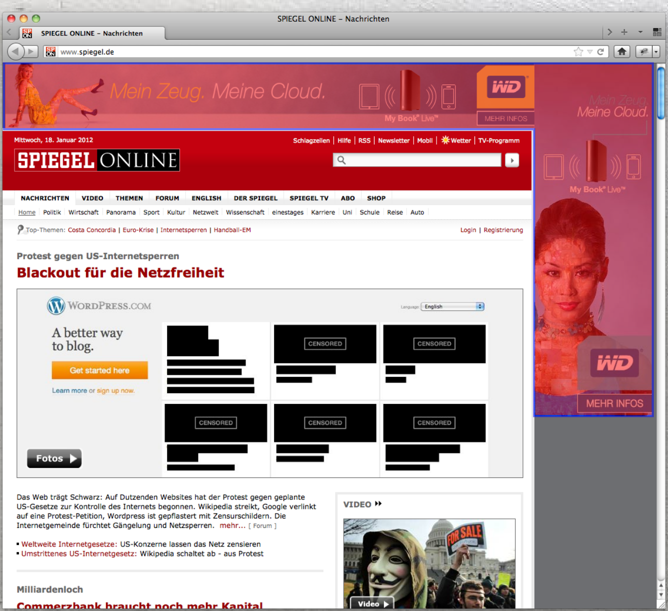
Das Web trägt Schwarz: Auf Dutzenden Websites hat der Protest gegen geplante US-Gesetze zur Kontrolle des Internets begonnen. Wikipedia streikt, Google verlinkt auf eine Protest-Petition, Wordpress ist gepflastert mit Zensurschildern. Die Internetgemeinde fürchtet Gängelung und Netzsperren. mehr... [Forum]

- Weltweite Internetgesetze: US-Konzerne lassen das Netz zensieren
- Umstrittenes US-Internetgesetz: Wikipedia schaltet ab - aus Protest

Milliardenloch

Commerzbank braucht noch mehr Kapital

Situation of a Web Programmer



Mittwoch, 18. Januar 2012

Top-Themen: Costa Concordia | Euro-Krise | Internetsperren | Handball-EM

Protest gegen US-Internetsperren

Blackout für die Netzfreiheit

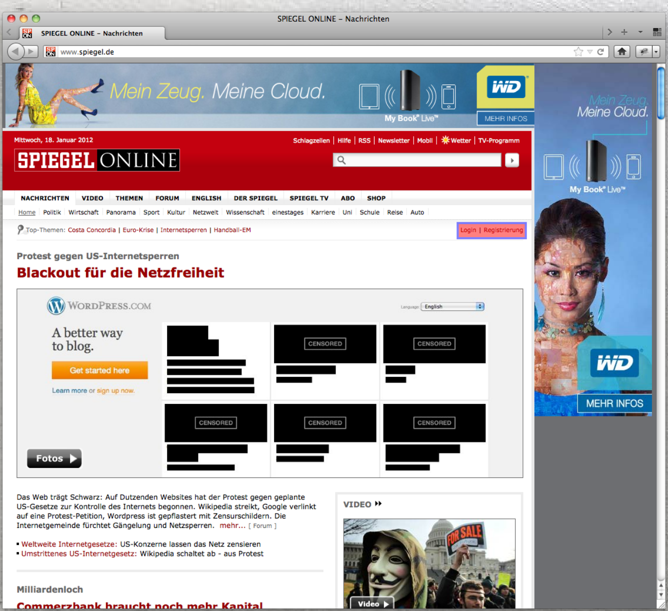
Das Web trägt Schwarz: Auf Dutzenden Websites hat der Protest gegen geplante US-Gesetze zur Kontrolle des Internets begonnen. Wikipedia streikt, Google verlinkt auf eine Protest-Petition, Wordpress ist geplastert mit Zensurschildern. Die Internetgemeinde fürchtet Gängelung und Netzsperren. mehr... [Forum]

- Weltweite Internetgesetze: US-Konzerne lassen das Netz zensieren
- Umstrittenes US-Internetgesetz: Wikipedia schaltet ab - aus Protest

Milliardenloch

Commerzbank braucht noch mehr Kapital

Situation of a Web Programmer



SPIEGEL ONLINE – Nachrichten
www.spiegel.de
Mein Zeug. Meine Cloud.
My Book® Live™
WD
MEHR INFOS
Mittwoch, 18. Januar 2012
Schlagzeilen | Hilfe | RSS | Newsletter | Mobil | Wetter | TV-Programm
SPIEGEL ONLINE
NACHRICHTEN VIDEO THEMEN FORUM ENGLISH DER SPIEGEL SPIEGEL TV ABO SHOP
Home Politik Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft einestages Karriere Uni Schule Reise Auto
Top-Themen: Costa Concordia | Euro-Krise | Internetsperren | Handball-EM
Login | Registrierung
WordPress.com
Language English
A better way to blog.
Get started here
Learn more or sign up now.
CENSORED
CENSORED
CENSORED
CENSORED
CENSORED
Fotos
VIDEO
FOR SALE
Video

Protest gegen US-Internetsperren

Blackout für die Netzfreiheit

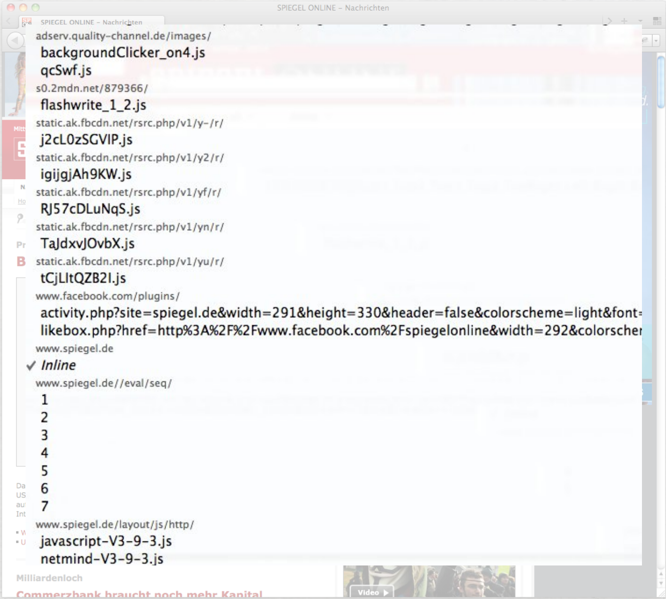
Das Web trägt Schwarz: Auf Dutzenden Websites hat der Protest gegen geplante US-Gesetze zur Kontrolle des Internets begonnen. Wikipedia streikt, Google verlinkt auf eine Protest-Petition, Wordpress ist gepflastert mit Zensurschildern. Die Internetgemeinde fürchtet Gängelung und Netzsperren. mehr... [Forum]

- Weltweite Internetgesetze: US-Konzerne lassen das Netz zensieren
- Umstrittenes US-Internetgesetz: Wikipedia schaltet ab - aus Protest

Milliardenloch

Commerzbank braucht noch mehr Kapital

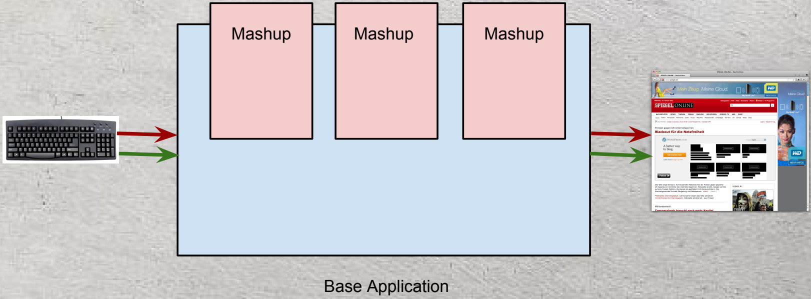
Situation of a Web Programmer



SPIEGEL ONLINE – Nachrichten
SPIEGEL ONLINE – Nachrichten
Milliardenloch
Commerzbank braucht noch mehr Kapital
Video

adserv.quality-channel.de/images/
backgroundClicker_on4.js
qcSwf.js
s0.2mdn.net/879366/
flashwrite_1_2.js
static.ak.fbcdn.net/rsrc.php/v1/y-/r/
j2cL0zSGVIP.js
static.ak.fbcdn.net/rsrc.php/v1/y2/r/
igijgjAh9KW.js
static.ak.fbcdn.net/rsrc.php/v1/yf/r/
RJ57cDLuNqS.js
static.ak.fbcdn.net/rsrc.php/v1/yn/r/
TaJdxvJOvbX.js
static.ak.fbcdn.net/rsrc.php/v1/yu/r/
tCjLItQZB2I.js
www.facebook.com/plugins/
activity.php?site=spiegel.de&width=291&height=330&header=false&colorscheme=light&font=
likebox.php?href=http%3A%2F%2Fwww.facebook.com%2Fspiegelonline&width=292&colorscher
www.spiegel.de
✓ *Inline*
www.spiegel.de//eval/seq/
1
2
3
4
5
6
7
www.spiegel.de/layout/js/http/
javascript-V3-9-3.js
netmind-V3-9-3.js

Visualization of the Code



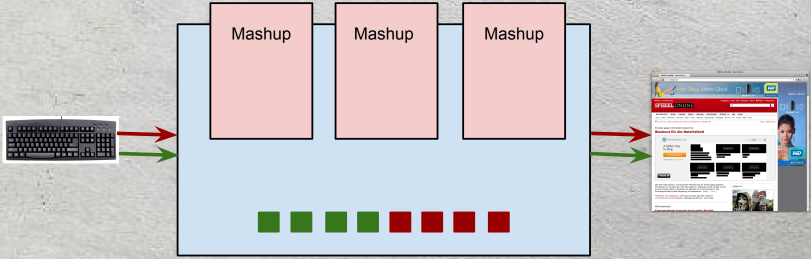
Mashup

Mashup

Mashup

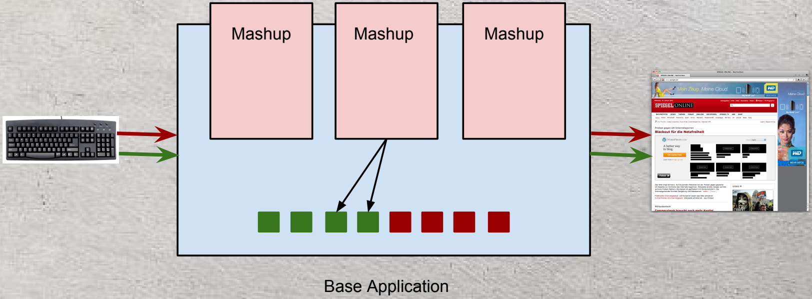
Base Application

Visualization of the Code

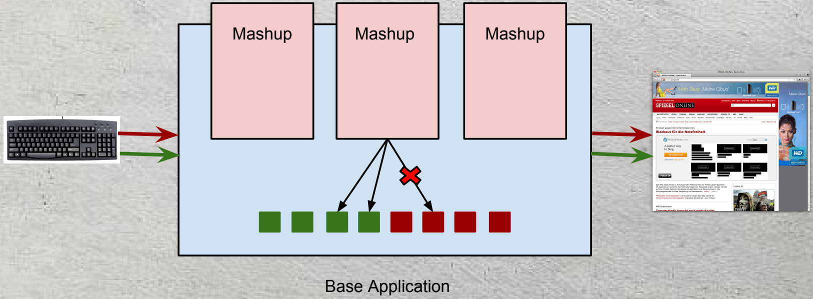


Base Application

Visualization of the Code



Visualization of the Code



Mashup

Mashup

Mashup

Base Application

Problem

(Mandatory) Access Control for Mashups

- No access to private data of the client
- No access to sensitive resources

Problem

(Mandatory) Access Control for Mashups

- No access to private data of the client
- No access to sensitive resources

What is Needed?

- Demarcation between trusted and untrusted code
- Mashup-specific access-control policies
- Enforcement of these policies

Observation

In JavaScript, every resource is controlled by reading or writing a property in scope.

Examples

- `document.location`, `document.cookie`, ...
- `document.write()`, ...
- `window.onload`, `window.onkeypress`, ...
- `window.alert()`, `window.open()`, ...
- `node.data`, `node.innerHtml`, ...
- `myData.contacts.JohnDoe.email`, ...

Controlling Access to Properties is Key!

Access Permissions — sets of object references

```
Perm (document, "location|cookie|write");
Perm (window, "/on.*/");
Perm (window, "alert|open");
Perm (document.documentElement, "*./data|innerHtml/");
Perm (myData, "*.email");
```

Controlling Access to Properties is Key!

Access Permissions — sets of object references

```
Perm (document, "location|cookie|write");
Perm (window, "/on.*/");
Perm (window, "alert|open");
Perm (document.documentElement, "*./data|innerHtml/");
Perm (myData, "*.email");
```

Building blocks

$$
\begin{array}{rcll}
p & ::= & \mathtt{Perm}(e, \mathit{path}) & \text{anchored path set} \\
 & | & p \cup p \mid p \cap p \mid \neg p & \text{boolean operations} \\
 & | & \Omega & \text{universal permission}
\end{array}
$$

Enforcing Restrictions

Enforcing Restrictions

```
ENFORCE( Deny (Perm (...), Perm (...)),
  function () {
    // scope of enforcement
  });
```

Alternative: Permitted Accesses

Access Permissions

```
/* constructor for person */
function Person(nick, pass, mail) {
  this.nickname = nick;
  this.password = pass;
  this.email    = mail;
}

function base_functionality() {
  var p = new Person("honda", "t243v3r", "mh@t2.com");
  ...
  ENFORCE( Allow (Perm (p, "nickname")),
    function() { mashup1 (p); });
  ...
  var out = document.getElementById("for_mashup");
  ENFORCE( Allow (Perm (out, "*")),
    function() { mashup2 (out, ...); });
}
```

Discussion: Scope of Enforcement

```
function mash(x, my) {
  ... my.secret ...
}

var r = ENFORCE(
  Deny(my, "secret"),
  function() {
    mash(x, my);
  });
```

Discussion: Scope of Enforcement

```
function mash(x, my) {
  ... my.secret ...
}

var r = ENFORCE(
  Deny(my, "secret"),
  function() {
    mash(x, my);
  });
```

Lexical Scope

- Restriction applies only to subphrases of `mash(x, my)`
- **Does not impose proper demarcation**: untrusted body of `mash` runs without restriction.

Discussion: Scope of Enforcement

```
function mash(x, my) {
  ... my.secret ...
}

var r = ENFORCE(
  Deny(my, "secret"),
  function() {
    mash(x, my);
  });
```

Dynamic Scope

- Restriction applies throughout execution of `mash`.
- Semantics of access permission contracts [POPL2012]

Discussion: Scope of Enforcement

```
function mash(x, my) {
  return function() {
    ... my.secret ...
  }
}

var r = ENFORCE(
  Deny(my, "secret"),
  function() {
    mash(x, my);
  });

r();// may access my.secret
```

Dynamic Scope

- Restriction applies throughout execution of `mash`.
- Semantics of access permission contracts [POPL2012]
- **Does not impose proper demarcation**:
  If the untrusted `mash` returned a function, then `r()`, i.e., code produced by `mash`, would run without restriction.

Discussion: Scope of Enforcement

```
function mash(x, my) {
  return function() {
  ... my.secret ...
  }
}

var r = ENFORCE(
  Deny(my, "secret"),
  function() {
    mash(x, my);
  });

r();
// no access to my.secret
```

Wrapper Semantics

- The restriction applies to the execution of `mash(x, y)` and to all functions and objects produced by it, recursively.
- If `mash(x, y)` returns a function, then the function call `r()` runs with (at least) the same restriction as `mash`.
- **Fits the requirements.**

Discussion: Scope of Enforcement

```
function mash(x, my) {
  ...  x()  ...
}

var r = ENFORCE(
  Deny(my, "secret"),
  function() {
    mash(x, my);
  });

// @syscall
function x() {
  ...  my.secret  ...
}
```

Wrapper Semantics for Higher-Order Functions

- Suppose `x` is a function, which is called in `mash`'s body.
- Which restriction applies to the execution of `x(...)`?
- Choice#1 (system call): `x`'s creation-time restriction

Discussion: Scope of Enforcement

```
function mash(x, my) {
  ... x()...
}

var r = ENFORCE(
  Deny(my, "secret"),
  function() {
    mash(x, my);
  });

// @callback
function x() {
  ... my.secret ...
}
```

Wrapper Semantics for Higher-Order Functions

- Suppose `x` is a function, which is called in `mash`'s body.
- Which restriction applies to the execution of `x(...)`?
- Choice#1 (system call): `x`'s creation-time restriction
- Choice#2 (callback): same plus the call-site's restriction

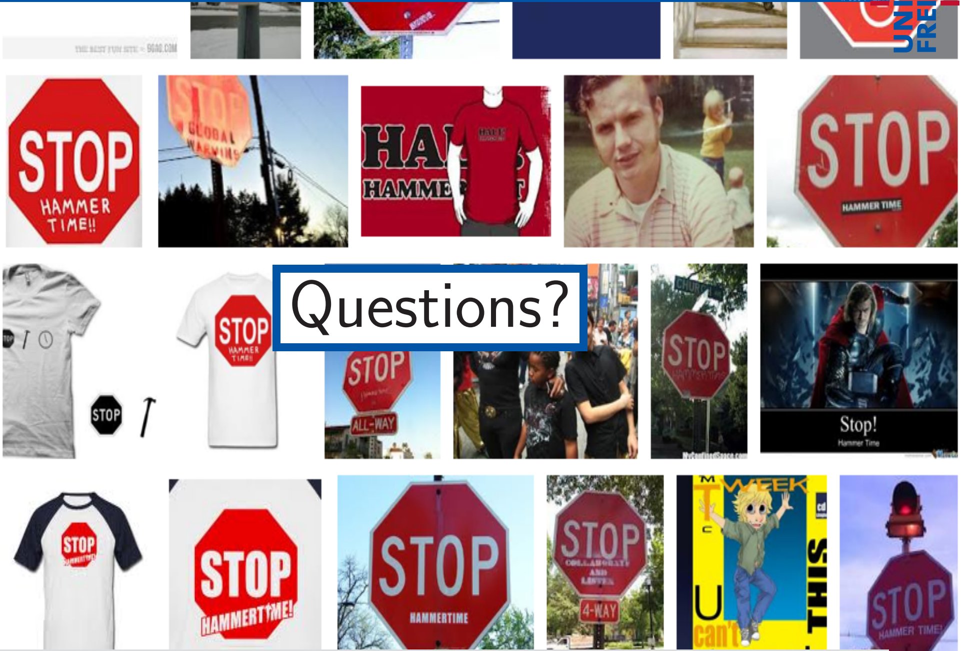
Who Should Use Access Restrictions?

- Implementer of base application wants to restrict mashups to guarantee confidentiality of the end user's data.
  - Explicit.
  - Instrumenting script tags.
- End user wants to restrict applications.
  - Global restriction.
  - Mapping: URL → restrictions.
  - Mapping prepared by third party; might be too complicated / tedious for end user.
- Implementer of mashup provides access restrictions: run time can check compatibility before executing

Project Status

- Formal, mechanized semantics
  - Properties of the semantics
  - Correctness of implementation
- Ongoing implementations in Rhino & Firefox
  - Security application requires total interposition
  - Only achievable in the JS engine (Thank you, eval & friends!)
- Corresponding gradual type system

The End



Questions?