

You Can't Touch This

HCSS Conference, Annapolis, MD

Albert-Ludwigs-Universität Freiburg

Manuel Geffken Peter Thiemann

University of Freiburg

thiemann@informatik.uni-freiburg.de

07 May 2013



UNI
FREIBURG

Motivation



Motivation



for application logic

on the client side

Concerns and Objective



Security & integrity

Security & integrity

Access control for JavaScript objects

- Domain specific language for specifying AC
- Dynamic analysis:
Enforcement of AC at run time
- Implementation as JavaScript library
+ extension of SpiderMonkey
- Planned: integration with static AC analysis

Composition of a Web Page



The screenshot shows a web browser window displaying the Spiegel Online website. The page features a navigation bar with categories like 'NACHRICHTEN', 'VIDEO', 'THEMEN', 'FORUM', 'ENGLISH', 'DER SPIEGEL', 'SPIEGEL TV', 'ABO', and 'SHOP'. A search bar is present in the top right. The main content area displays an article titled 'Protest gegen US-Internetsperren' with the sub-headline 'Blackout für die Netzfreiheit'. The article content is heavily redacted with black boxes and the word 'CENSORED'. A video player is visible at the bottom right of the article, showing a person in a Guy Fawkes mask. To the right of the article is a vertical advertisement for WD My Book Live, featuring a woman's face and the text 'Mein Zeug. Meine Cloud.' and 'MEHR INFOS'.

Composition of a Web Page



The screenshot shows a web browser window displaying the Spiegel Online website. The page features a red header with the site's name and navigation links. A main article is highlighted with a blue border, titled "Protest gegen US-Internetsperren" and "Blackout für die Netzfreiheit". The article content is partially obscured by red boxes labeled "CENSORED". Below the article, there is a "VIDEO" section with a thumbnail of a person holding a "FOR SALE" sign. The right side of the page has a vertical sidebar with a woman's face and a "WD" logo.

SPiegel ONLINE - Nachrichten
www.spiegel.de

Mein Zeug. Meine Cloud.
My Book* Live™

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

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

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

Protest gegen US-Internetsperren
Blackout für die Netzfreiheit

WORDPRESS.COM
A better way to blog.
Get started here
Learn more or sign up now.

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 Netzperren. mehr... [Forum]

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

Milliardenloch
Commerzbank braucht noch mehr Kapital

VIDEO ▶
Video ▶

Mein Zeug. Meine Cloud.
My Book* Live™
MEHR INFOS

Composition of a Web Page



The screenshot shows a web browser window displaying the Spiegel Online website. The page features a red header with the site's logo and navigation menu. The main content area is titled "Protest gegen US-Internetsperren" and "Blackout für die Netzfreiheit". It includes a WordPress.com advertisement with a "A better way to blog." message and several blacked-out sections labeled "CENSORED". A video player at the bottom shows a person in a Guy Fawkes mask. The right sidebar contains a "Meine Cloud" advertisement and a "WD" logo.

Mein Zeug. Meine Cloud.

My Book* Live*

MEHR INFOS

Mitwoch, 18. Januar 2012

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

SPIEGEL ONLINE

NACHRICHTEN VIDEO THEMEN FORUM ENGLISH DER SPIEGEL SPIEGEL TV ABO SHOP

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

A better way to blog.

Get started here

Learn more or sign up now.

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 Netzsperrn. mehr... [Forum]

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

Milliardenloch

Commerzbank braucht noch mehr Kapital

VIDEO ▶

WD

MEHR INFOS

Composition of a Web Page



The screenshot shows a web browser window displaying the Spiegel Online news website. The page features a red header with the site's logo and navigation links. A main article titled "Protest gegen US-Internetsperren" is visible, with a sub-headline "Blackout für die Netzfreiheit". Below the article, there is a section for a WordPress advertisement that has been heavily censored with black boxes and the word "CENSORED". To the right of the main content, there is a vertical advertisement for WD My Book Live, featuring a woman's face and the WD logo. The browser's address bar shows "www.spiegel.de".

SPiegel ONLINE - Nachrichten

www.spiegel.de

Mein Zeug. Meine Cloud.

My Book® Live™

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

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

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

Login | Registrierung

Protest gegen US-Internetsperren
Blackout für die Netzfreiheit

WordPress.com

A better way to blog.

Get started here

Learn more or sign up now.

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 Netzsperrern. mehr... [Forum]

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

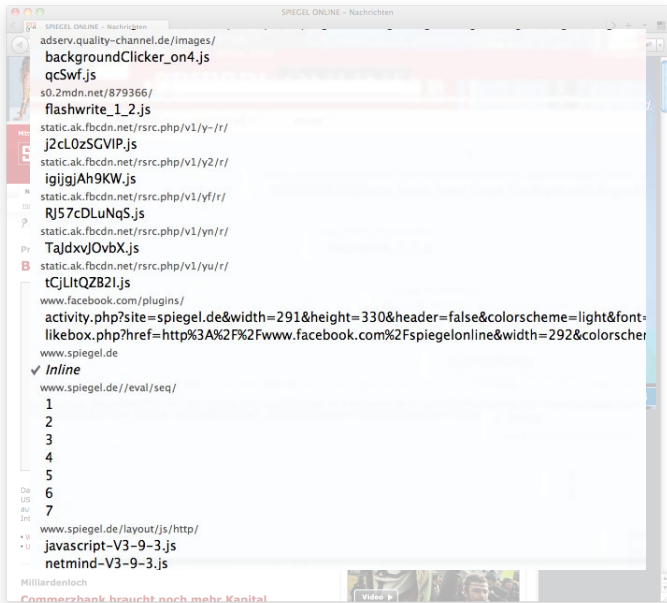
Milliardenloch

Commerzbank braucht noch mehr Kapital

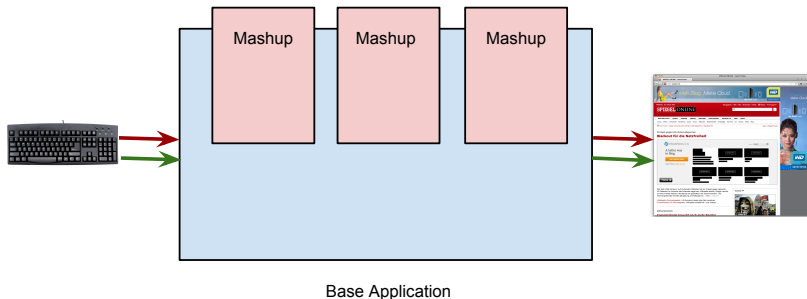
VIDEO

Video

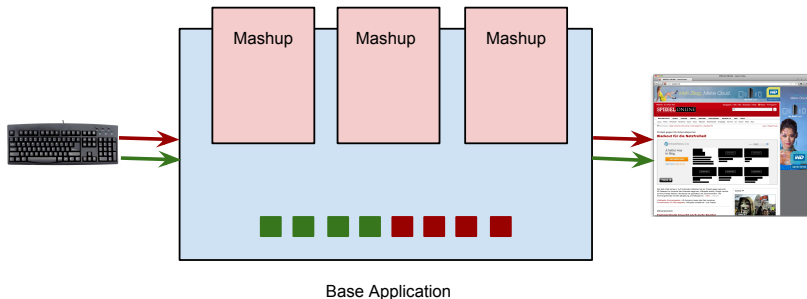
Composition of a Web Page

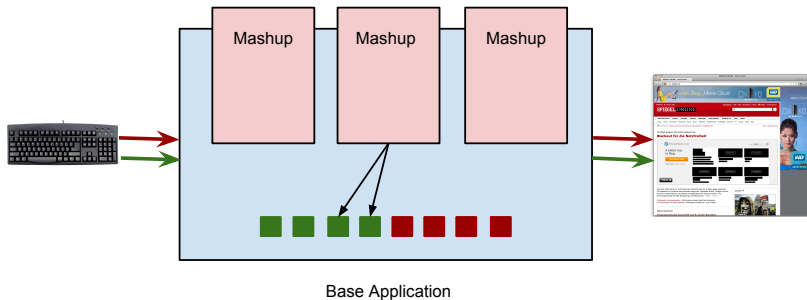


Visualization of the Code

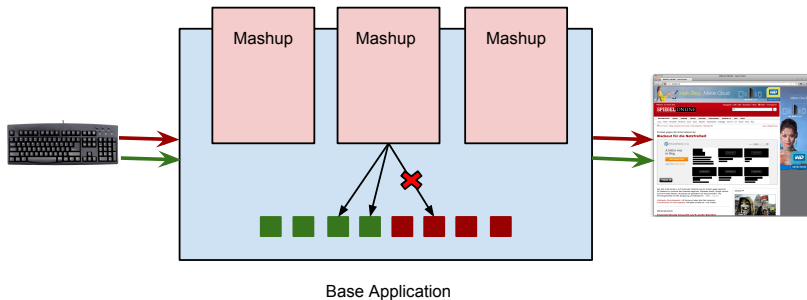


Visualization of the Code





Visualization of the Code



(Mandatory) Access Control for Mashups

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

(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

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

Examples

- `document.location`, `document.cookie`, ...
- `window.onload`, `window.onkeypress`, ...
- `node.data`, `node.innerHTML`, ...
- `myData.contacts.JohnDoe.email`, ...



Basic permissions — sets of object references

```
Read (document, "location|cookie");  
Read (window, "onload|onkeypress");  
Write(document.documentElement, "*(data|innerHTML)");  
Read (myData, "*.email");
```

Basic permissions — sets of object references

```
Read (document, "location|cookie");  
Read (window, "onload|onkeypress");  
Write(document.documentElement, "*(data|innerHTML)");  
Read (myData, "*.email");
```

Building blocks – path sets

$a ::=$	$\text{Read}(e, path) \mid \text{Write}(e, path)$	anchored path set
	$\text{Join}(a, a) \mid \text{Meet}(a, a) \mid \text{Not}(a)$	boolean operations
	All	universal permission

- $M : \text{AP expression} \rightarrow \mathbb{P}(\text{Loc} \times \text{Prop}) \times \mathbb{P}(\text{Loc} \times \text{Prop})$
read and write components
- $M(\text{Read}(\ell, p)) = (\{(\ell, p)\}, \{\})$
singleton read set
- $M(\text{Write}(\ell, p)) = (\{\}, \{(\ell, p)\})$
singleton write set
- $M(\text{Join}(a_1, a_2)) = M(a_1)(\cup \times \cup)M(a_2)$
componentwise union
- $M(\text{Meet}(a_1, a_2)) = M(a_1)(\cap \times \cap)M(a_2)$
componentwise intersection
- $M(\text{Not}(a)) = (\text{Loc} \times \text{Prop}, \text{Loc} \times \text{Prop}) \setminus M(a)$
componentwise negation
- $M(\text{All}) = (\text{Loc} \times \text{Prop}, \text{Loc} \times \text{Prop})$



DSL: Enforcement of APs

ENFORCE takes two parameters

- AP expression describing read set R and write set W
- thunk executed under dynamic monitoring of R and W



Enforcing Access Permissions

DSL: Enforcement of APs

ENFORCE takes two parameters

- AP expression describing read set R and write set W
- thunk executed under dynamic monitoring of R and W

Example: Withdrawing Access Permissions

```
ENFORCE( Not (Join ( Read (...), Write (...))),  
function () {  
    // scope of enforcement  
});
```

Example: Granting Access Permissions

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

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

Discussion: Scope of Enforcement

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

```
var r = ENFORCE( Not(  
  Read(my, "secret")),  
  function () {  
    mash(x, my);  
  });
```


Discussion: Scope of Enforcement

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

```
var r = ENFORCE( Not(  
  Read(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( Not(  
  Read(my, "secret")),  
  function () {  
    mash(x, my);  
  });
```

Dynamic Scope

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

Discussion: Scope of Enforcement

```

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

var r = ENFORCE( Not(
  Read(my, "secret")),
  function() {
    mash(x, my);
  });

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

Dynamic Scope

- Restriction applies during 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.

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

```
var r = ENFORCE( Not(  
  Read(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.**

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

```
var r = ENFORCE( Not(  
  Read(my, "secret")),  
  function() {  
    mash(x, my);  
  });
```

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

Wrapper Semantics for Higher-Order Functions

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

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

```
var r = ENFORCE( Not(  
  Read(my, "secret")),  
  function () {  
    mash(x, my);  
  });
```

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

Wrapper Semantics for Higher-Order Functions

- Suppose x is a function 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

- 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

- Integration in Spidermonkey / Firefox
 - Security application requires total interposition
 - Only achievable in the JS engine (Thank you, eval & friends!)
- DSL implementation and object traversal in JavaScript
- Result: set of objects with permissions
- Interception of read and write operations in Spidermonkey
- Problems
 - set must be a weak set hashed with object identities
 - only available in the latest version of Spidermonkey
 - interface JavaScript vs. implementation language C++

- Mechanized formal semantics
 - Properties of the semantics
 - Correctness of implementation
- Ongoing implementation in Spidermonkey / Firefox
- Corresponding gradual type system
 - in development
 - integrates statically typed and dynamically checked code

The End



Questions?