

Secure Mashups with OpenAjax Hub 1.1 and OpenAjax Widget Metadata

Jon Ferraiolo

IBM and OpenAjax Alliance

July 23, 2008

Agenda

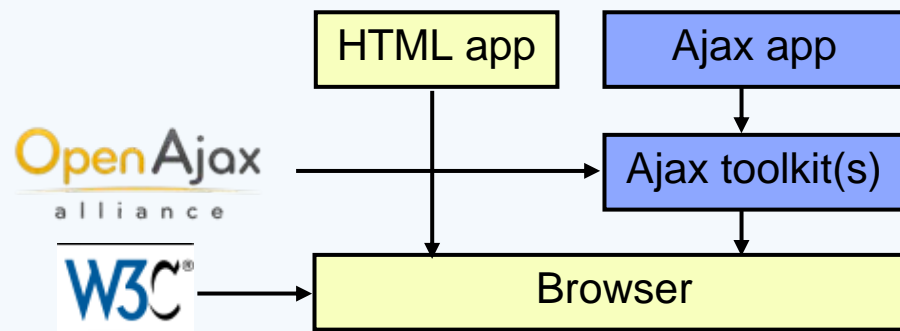
- **Introducing OpenAjax Alliance**
- **Introduction to Mashups**
- **OpenAjax Hub1.0**
- **OpenAjax Hub 1.1**
- **OpenAjax Metadata for Widgets**
- **Demo**
- **Summary**

The Ajax explosion (2005-2007)

- Huge amount of hype
- ~200 Ajax toolkits appear almost instantly
 - Microsoft Atlas (now called ASP.NET AJAX)
 - *Helps contribute to legitimacy*
 - Several other major “proprietary” Ajax frameworks
 - *Adobe/Spry, Backbase, ICEsoft, Nexaweb, Sun/jMaki, TIBCO, ...*
 - Several major open source projects
 - *Prototype/Scriptaculous, Dojo, Yahoo, DWR, Google GWT, jQuery, ...*
 - Why so many so quickly? Simply rebrand DHTML to Ajax

Why OpenAjax Alliance?

- **A rich but fragile ecosystem**
 - Interoperability shortcomings
 - Educational/marketing shortcomings
 - Dependence on browsers companies for technical advances
- **Ajax vendors motivated to work together (united we stand, divided we fall)**
- **Ajax technology layer not addressed by other industry groups**



OpenAjax Alliance Formation

- **Kick-off meeting May 2006**
 - 30 companies
 - Objectives, process, scope, and initial tasks
- **Scope of activities**
 - Interoperability
 - Educational
 - Help shape the future of the Ajax ecosystem
- **What we produce**
 - Documents (e.g., specs)
 - Open source (mostly JavaScript)

OpenAjax Alliance Areas of Focus

- **Interoperability**
 - Ajax runtime libraries
 - Ajax IDEs
 - Mashups and widgets
 - Mobile Ajax
- **Marketing, education and evangelism**
- **Future browsers**

Runtime Interoperability

- Runtime = JavaScript running in the browser
- Problems
 - Name collisions
 - Integration difficulties
 - *Critical for mashups, where you assemble pre-built components onto the canvas, often using different Ajax toolkits*
- OpenAjax Registry
 - An industry-wide registry of JavaScript globals, CSS classnames, and HTML markup extensions
- OpenAjax Hub
- OpenAjax Metadata

IDE Interoperability

- IDEs = Developer tools (code assist, debug, visual layout)
- Problem
 - NxM permutation problem (~200 Ajax toolkits, ~15 Ajax IDEs)
 - Each Ajax toolkit documents their APIs and widgets in their own way
- **OpenAjax Metadata for Ajax Libraries**
 - Industry standard XML for:
 - *JavaScript APIs*
 - *UI controls*
- **OpenAjax Alliance's IDE WG members**
 - Adobe Dreamweaver
 - Eclipse (Aptana, JSDT, ATF0)
 - Microsoft Visual Studio

Mashup and Widget Interoperability

- Mashups = Ability to assemble pre-built components into a composite application
- Problems
 - Security
 - Widget interoperability
- OpenAjax Hub 1.1
- OpenAjax Metadata for Widgets
- Open source widget transcoders
- Open source mini-mashup tool

Mobile Ajax

- **Mobile Ajax = Full Ajax running on mobile phones**
- **Problems**
 - Special challenges (screen size, latency, keypad, battery, ...)
 - Special opportunities (portability, GPS, camera, voice, ...)
- **White paper: Introduction to Mobile Ajax for Developers**
- **Mobile Device APIs**
 - Open source JavaScript to access CPS, camera, address book, SMS, ...
 - Targets both existing proprietary, system-dependent APIs (via plugins) and emerging industry standards
 - Collaborating with OMTP, tracking W3C (e.g., geolocation)

Marketing, Education and Evangelism

- **Problems:**
 - Industry: needs a central place for industry-wide initiatives
 - Customers: With so many choices: Ajax can be confusing to newcomers
- **OpenAjax Conformance**
 - A small set of conformance requirements that products must meet in order to interoperate well with other Ajax products
 - An Ajax industry interoperability trust brand
- **White papers**
 - Introduction to Ajax and OpenAjax
 - When Does Ajax Make Business Sense
 - Next Generation Applications Using Ajax and OpenAjax
 - Successful Deployment of Ajax and OpenAjax
 - Ajax and Mashup Security
 - Introduction to Mobile Ajax for Developers
 - Good News for Ajax – the Browser Wars are Back

Shaping the Future of Ajax Ecosystem

- **Ajax industry browser wishlist initiative**
 - April – July, 2008
 - 222 participants, including many industry leaders
 - 55 separate feature requests described and discussed on wiki
- **Top feature requests**
 - 2D Graphics
 - Security (better prevention of XSS and CSRF)
 - Improved low-level DOM hooks for visual layout
 - DOM performance
 - Rich text editing
 - Server push (Comet)
 - Video and audio

Agenda

- Introducing OpenAjax Alliance
- Introduction to Mashups
- OpenAjax Hub1.0
- OpenAjax Hub 1.1
- OpenAjax Metadata for Widgets
- Demo
- Summary

Business value of mashups



- **Faster, cheaper delivery of applications**
 - Save time and money through reuse and lightweight integration techniques
 - Lower skill set needed to assembly new applications
- **Support innovation and new business opportunities**
 - Users empowered to innovate and explore
- **Gain valuable insights**
 - Due to remixing enterprise and web information
- **Better align IT and business**
 - Do-it-yourself IT will be expected by Facebook generation
- **Extend reach and value of SOA**
 - Service reuse illuminates the business value of SOA

Mashup software



- **Mashup tools**

- Widget and feed discovery
- Application assembly
- Instant deployment

- **Widgets**

- Pre-packaged, remixable mini-applications
- Usually tied to a back-end web service
 - Sometimes leveraging previous investment in SOA
- Public or company-private
- Key enabler of the long tail

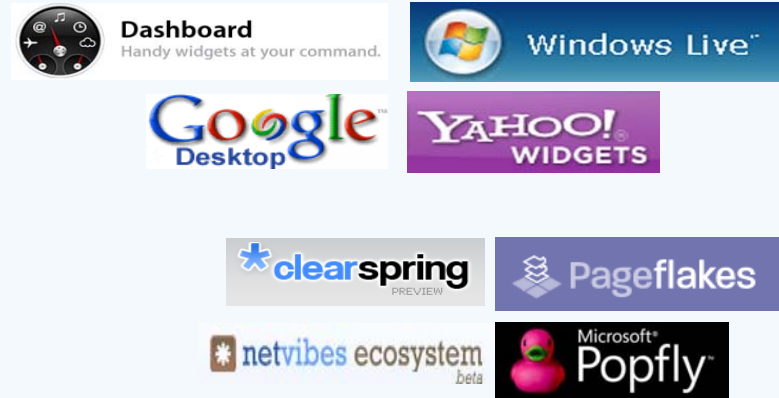
Widget innovation – no shortage



Industry challenges

■ Interoperability

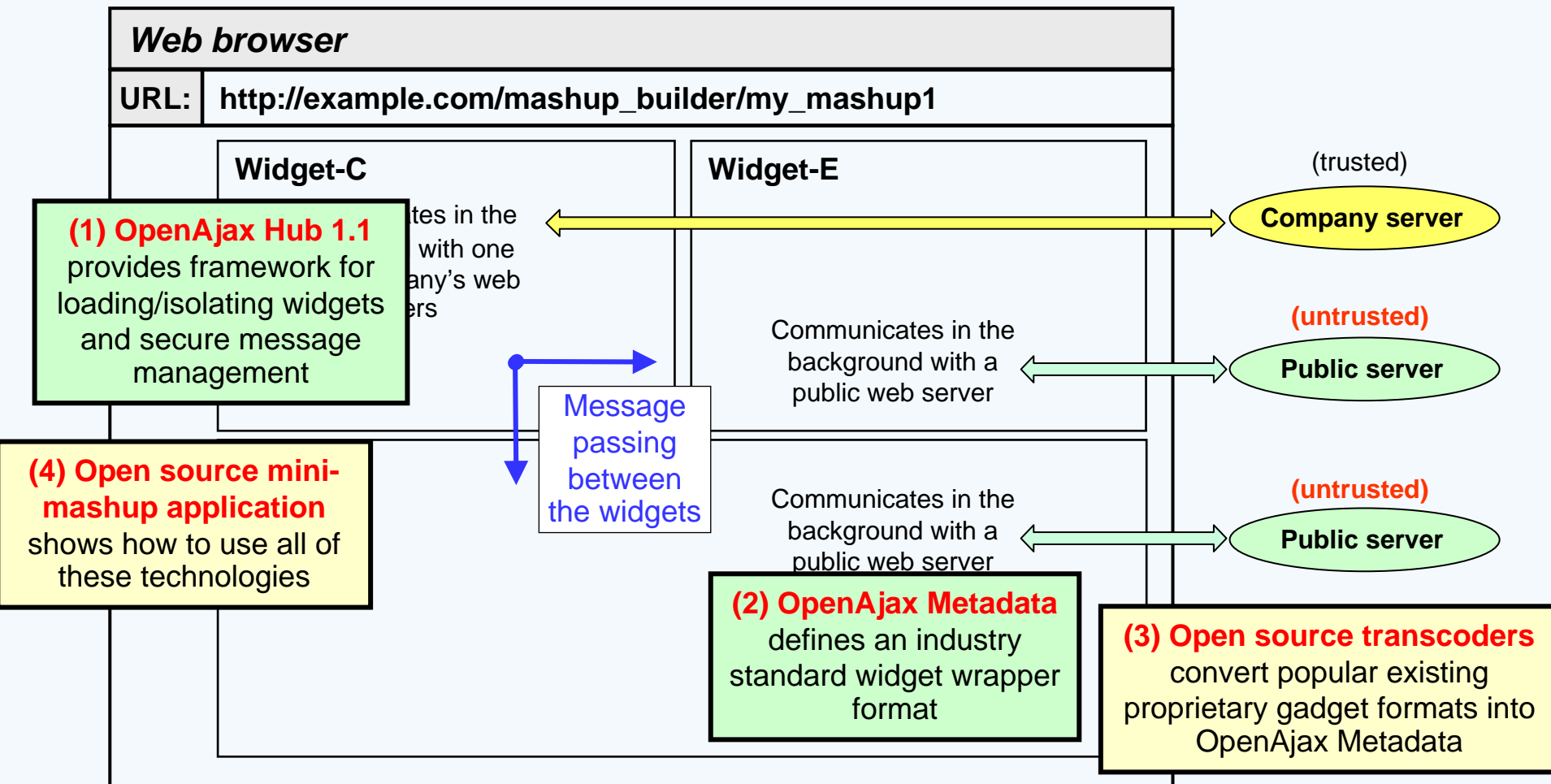
- Dozens of proprietary technologies
- *Good news: many use the "Web Runtime" (i.e., Ajax)!*
- Bad news: even when using the Web Runtime, widgets are not interoperable



■ Security

- The power of mashups – comes largely from discovering and integrating great widgets from 3rd parties
- But 3rd party widgets might be malicious

OpenAjax – Addressing the challenges



Agenda

- Introducing OpenAjax Alliance
- Introduction to Mashups
- OpenAjax Hub 1.0
- OpenAjax Hub 1.1
- OpenAjax Metadata for Widgets
- Demo
- Summary

OpenAjax Hub 1.0

- **What is it?**
 - Small bit of standard JavaScript (< 3K after compaction)
 - Enables multiple Ajax runtimes to work together
- **Key use case: *Developer mashups***
 - Where a professional developer mashes up components using HTML+JavaScript+...
- **Version 1.0 features**
 - Ajax library registration
 - *OpenAjax.hub.registerLibrary()*
 - Simple publish/subscribe engine (the pub sub hub)
 - *OpenAjax.hub.publish(topicName, payload)*
 - *OpenAjax.hub.subscribe(topicName, callbackFunction)*

OpenAjax Hub 1.0 – an example

Assume multiple Ajax toolkits:

- UTILS.js – Various utils, inc. XHR
- CALENDAR.js – Calendar control
- DATAGRID.js – Powerful tables
- CHARTS.js – Charting utilities

The visual controls need to react to new server data and to each other and update their views appropriately.

OpenAjax Hub 1.0 Example

This is a mockup of a Web application that uses UI controls from multiple Ajax toolkits.

| ContactName | ContactEmail | JobTitle | CompanyName | PhoneNumber | Address |
|----------------|----------------|----------------|-------------------|----------------|---------------------|
| Chong Marshaaa | s | sdfa | Forward Eagle Lt | 21313223 | 592 Honeywood |
| Arie Fields | BASKAR | fhghfaa | EclipseTorch Lic. | (894) 815-9624 | 943 Sleepy Mead |
| Klara Copeland | Klara Copeland | dfa | asdf | (445) 116-2746 | 47 Wallace Avenu |
| Brandy Gates | bgates@sfu.ca | VP Purchasing | asasdf | (563) 552-8487 | 542 Sleta Street, I |
| Reda Church | r_church@ebade | MR Coordinator | IdaTorch | (238) 853-7588 | 26 Dolly Avenue, I |
| Daria Sears | dsears@sfx.ca | asdf | CaliforniaResear | (774) 842-1947 | 24 Kiska Circle, F |

A Range of Things

The chart shows 'Areas' on the y-axis (ranging from min to max) and 'A Range of Things' on the x-axis (ranging from 0 to 100). The chart displays multiple data series with shaded areas representing ranges.

Example – under the hood

```
<html>
  <head>
    ...
    <script type="text/javascript" src="OpenAjax.js"/>
    <script type="text/javascript" src="UTILS.js"/>
    <script type="text/javascript" src="CALENDAR.js"/>
    <script type="text/javascript" src="CHARTS.js"/>
    <script type="text/javascript" src="DATAGRID.js"/>
    <script type="text/javascript">
      ...
      function MyCalendarCallback(...) {
        OpenAjax.hub.publish("myapp.newdate", newdate);
      }
      ...
      function NewDateCallback(eventname, publisherData, subscriberData) {
        ...update the given visualization widget...
      }
      OpenAjax.hub.subscribe("myapp.newdate", NewDateCallback);
      ...
    </script>
  </head>
  ...
```

OpenAjax InteropFest

- Objectives:
 - Allows OpenAjax Alliance to verify that OpenAjax Hub is reliable, performant, and suitable
 - Allows members to verify that they are OpenAjax Conformant

Jan-March 2007

OpenAjax Hub Basic Conformance Test - Mozilla Firefox

file:///C:/latest3/openajaxalliance/trunk/conformancetests/interopfest-2007-03/

OpenAjax alliance Standardizing Ajax Development

OpenAjax Hub Basic Conformance Test

For library: SampleAjaxLibrary

| | | |
|---|--|-------------------|
| 1 | OpenAjax Conformance Requirement (Libraries): Library Registration | TEST SUCCEEDED!!! |
| 2 | OpenAjax Conformance Requirement (Libraries): Globals Registration | TEST SUCCEEDED!!! |
| 3 | OpenAjax Conformance Requirement (Libraries): Load/Unload Handlers Registered Indirectly Through the Hub | TEST SUCCEEDED!!! |
| 4 | OpenAjax Hub Publish/Subscribe Test | TEST SUCCEEDED!!! |
| 5 | OpenAjax Hub Markup Scanner Test | TEST SUCCEEDED!!! |

12 toolkits participated
http://www.openajax.org/member/wiki/InteropFest_2007_March

July-Sept 2007

InteropFest 1.0 Example Web Page - Mozilla Firefox

file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/Software/InteropFest10/index.html

InteropFest 1.0 Example Web Pa...

OpenAjax alliance Standardizing Ajax Development

OpenAjax Alliance InteropFest 1.0 Template

About this template

This page is a template for InteropFest 1.0 that culminates at the OpenAjax Alliance face-to-face meeting on Sept 21, 2007. To participate in the InteropFest, you need to customize this template per the instructions that begin with the README.txt file that accompanies this template.

The only part of this template that must be preserved after your customizations is the results table that you see in the lower-left corner. It is OK to re-use the results table and/or put it in a different location.

Your customizations can also remove/replace the OpenAjax banner at the top of the page, but you must preserve the smaller-size banner that sits on top of the test results.

No matter how you customize, remove or replace this section.

OpenAjax alliance Standardizing Ajax Development

OpenAjax InteropFest 1.0 Test Results

| | |
|---------------------------|-----------------|
| Library registration test | TEST SUCCESSFUL |
| Pub/sub test | TEST SUCCESSFUL |
| # Registered libraries | 3 |
| # Messages published | 1516 |
| # Messages received | 1516 |
| # Unique topics received | 3 |

Data generation component

NOTE: This template uses a client-side JavaScript component to generate random stock value change events. As the README.txt file explains, there are many options for customizing this template. Among the options: (1) you can use the datagen component, (2) you can replace the datagen component, or (3) you can customize in more radical ways. Whatever you decide, as part of your customization effort, remove this paragraph.

Click the buttons below to pause or resume the continuous feeds of simulated stock market price changes.

Pause

Data visualization component

NOTE: This template uses a client-side JavaScript component to use an HTML table to present the stock value change events. As the README.txt file explains, there are many options for customizing this template. Among the options: (1) you can use this simple data viz component, (2) you can replace the data viz component, or (3) you can customize in more radical ways. Whatever you decide, as part of your customization effort, remove this paragraph.

| | | |
|---------------------------|------|--------|
| East Bay Electric | EBEL | 91.12 |
| Stall Systems | SLSY | 89.12 |
| Lattent Circuits | LATR | 87.14 |
| Vesarian Executive Search | VEOS | 114.14 |
| Steerberry Computers | STRA | 87.12 |
| Titan Perseer | TITA | 90.14 |
| Clusoft Systems | CLSO | 108.12 |
| West Pacific Inc. | WPSI | 85.12 |

14 organizations, 20 toolkits participated
http://www.openajax.org/member/wiki/InteropFest_1.0

InteropFest Demos

For people who are just looking at the slide deck, some InteropFest demos can be found at:

- http://www.openajax.org/member/wiki/InteropFest_1.0

| Participating organizations | Participating toolkits |
|-----------------------------|------------------------------|
| 24SevenOffice | AjaxEngine |
| Apache XAP | Apache XAP |
| Dojo Foundation | Dojo Toolkit |
| IBM | Ext |
| ILOG | ILOG JViews |
| DWR/Getahead | IT Mill Toolkit |
| IT Mill | jMaki |
| Lightstreamer | JQuery |
| Microsoft | Lightstreamer |
| Nexaweb | Microsoft Ajax Library |
| OpenLink SW | Nexaweb Ajax Client |
| Open Spot | OAT: OpenLink AJAX Toolkit |
| Software AG | OpenSpot CalcDesk |
| Sun Microsystems | Prototype |
| TIBCO | script.aculo.us |
| | Software AG's webMethods/CAF |
| | TIBCO General Interface |
| | 24SevenOffice Vili |
| | YUI |

OpenAjax Hub 1.0

- **Status**
 - *Approved*
- **Specification**
 - http://www.openajax.org/member/wiki/OpenAjax_Hub_1.0_Specification
- **Reference implementation at SourceForge**
 - <http://openajaxallianc.sourceforge.net>

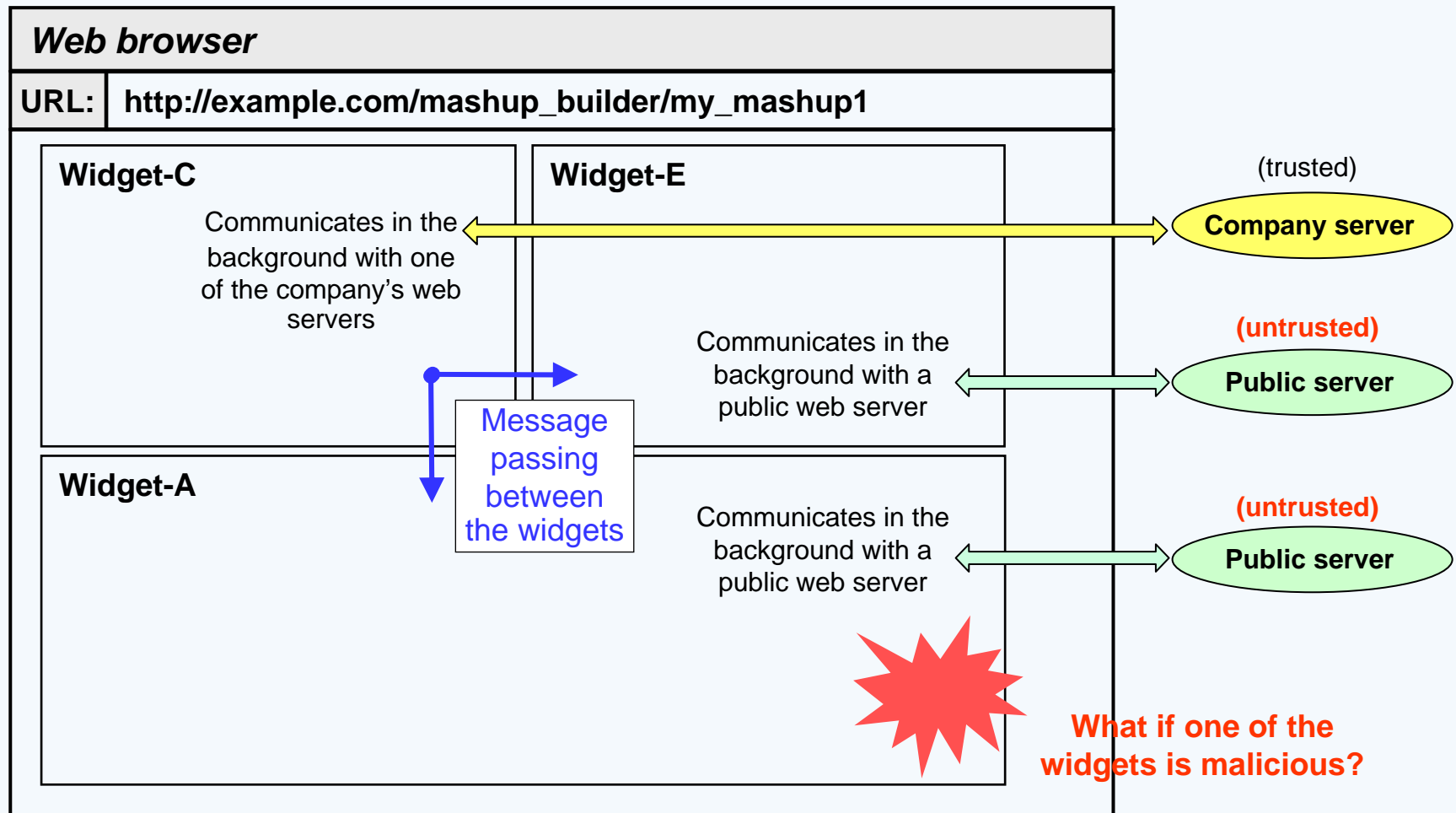
Agenda

- Introducing OpenAjax Alliance
- Introduction to Mashups
- OpenAjax Hub1.0
- OpenAjax Hub 1.1
- OpenAjax Metadata for Widgets
- Demo
- Summary

OpenAjax Hub 1.1 – New features

- OpenAjax Hub 1.0
 - Key use case: *Developer mashups*
 - Key technology: pub/sub within a single browser frame
- OpenAjax Hub 1.1
 - Key use case: *Secure end-user mashups*
 - Key technologies
 - *Widget isolation (for security)*
 - *Pub/sub across browser frames*
 - *Security manager mediates all cross-widget messages*

Security vulnerabilities



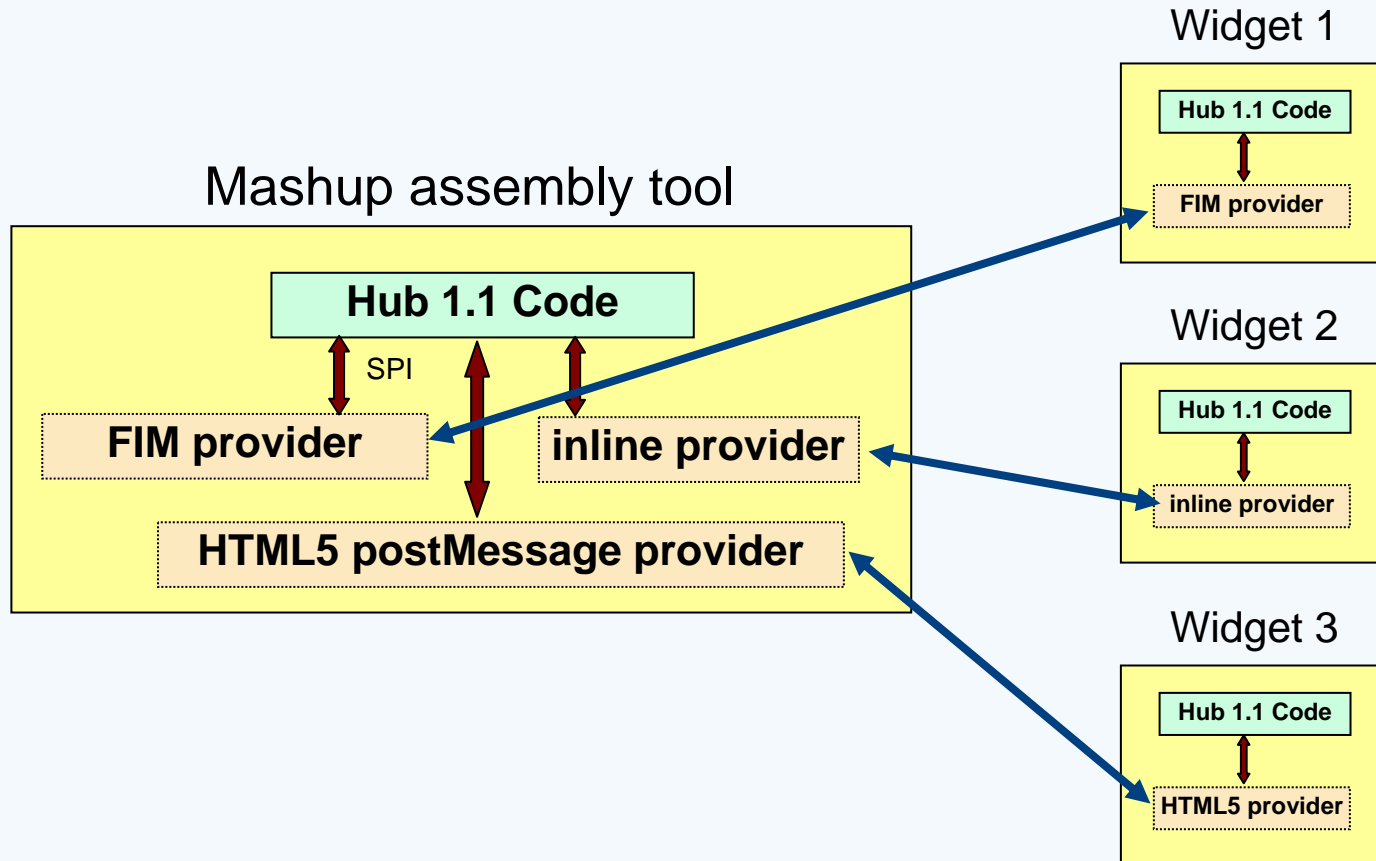
Browser Security

- **Browser same-origin policy**
 - IFRAMEs isolation - IFRAMEs from different domains (and subdomains) cannot communicate with each other via DOM bridging or JavaScript bridging
 - Implemented in all popular Web browsers today
- **Today's tricks for cross-domain mashups**
 - Dynamic SCRIPT tag to another server
 - Server-side proxies
 - "IFrame proxy" (window.location fragment identifier)
 - New browsers: W3C postMessage() and Access Control

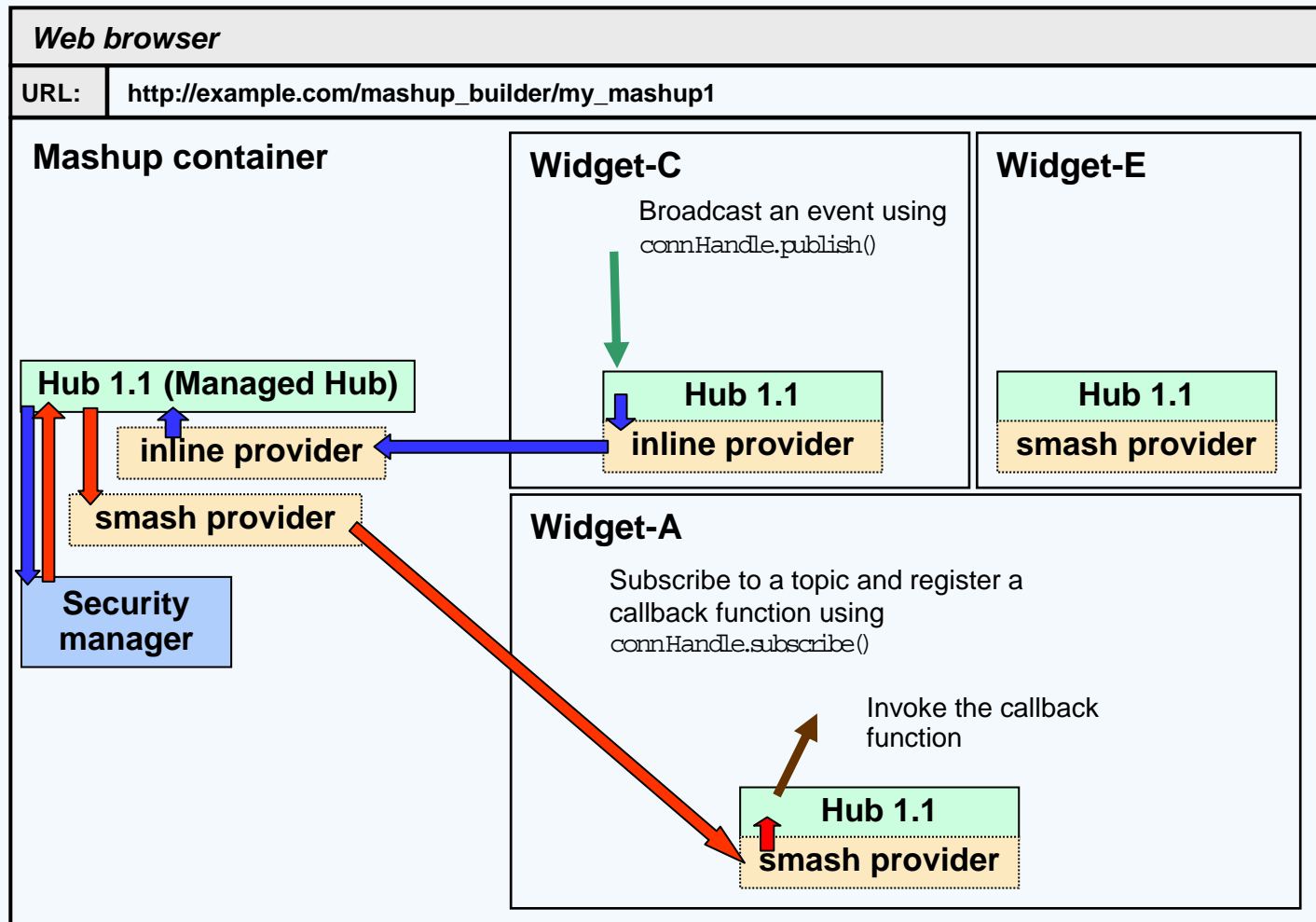
SMash

- **SMash stands for “Secure Mashups”**
 - Secure handling of 3rd party mashup components
 - Runs in today’s browsers (without plugins)
- **Designed and implemented at IBM™ Research (beginning of 2007)**
 - Open-sourced (openajaxalliance.sourceforge.net) in August 2007
 - Research Paper describing SMash in WWW 2008 Conference
- **High-level APIs, independent of implementation technology**
 - Fragment communication, HTML5 postMessage, Java™ platform, Flash etc.
 - Will still work when browsers add native support for secure cross-frame messaging

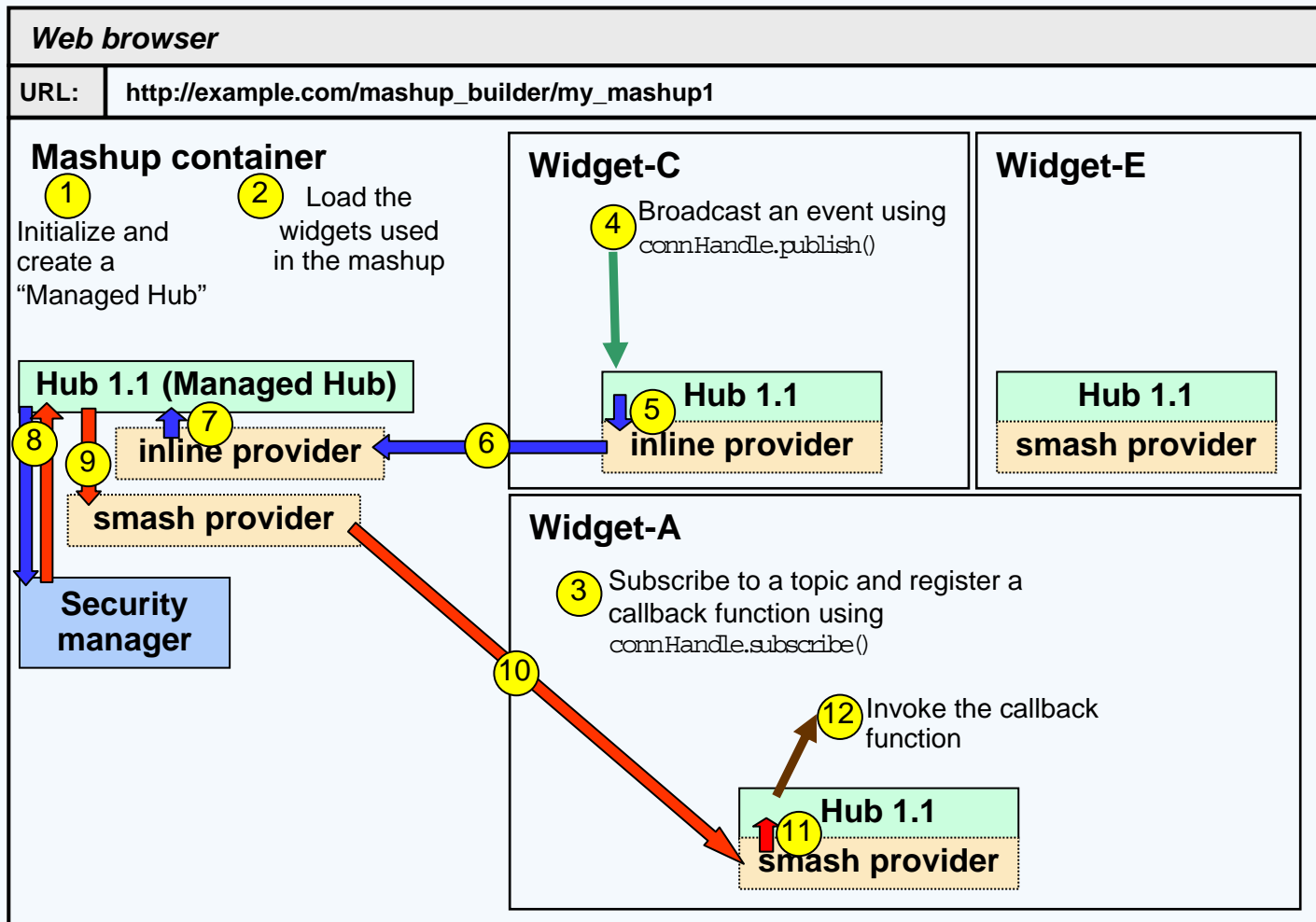
OpenAjax Hub 1.1: Plug-in communication providers



OpenAjax Hub 1.1: Simple example



OpenAjax Hub 1.1: the steps



Hub 1.1 status

- **Specification**
 - First draft spec – far along
 - http://www.openajax.org/member/wiki/OpenAjax_Hub_1.1_Specification
- **Reference implementation at SourceForge**
 - First implementation (far along)
 - <http://openajaxallianc.sourceforge.net>
- **Timeline for Hub 1.1**
 - July-September 2008: 2008 InteropFest
 - Fall 2008: Finalize and approve

Agenda

- Introducing OpenAjax Alliance
- Introduction to Mashups
- OpenAjax Hub1.0
- OpenAjax Hub 1.1
- OpenAjax Metadata for Widgets
- Demo
- Summary

Widget innovation – no shortage



OpenAjax Metadata

- **Mashup shortcomings today**
 - Widget interoperability
 - *Many widget formats (Google, Yahoo, Apple, Microsoft...)*
 - *Widget developers usually have to build different versions of their widgets to work with different containers*
 - Security
 - *No comprehensive, standards-based approach to widget isolation*

- **OpenAjax Metadata addresses these two shortcomings**
 - Widget interoperability
 - *OpenAjax Metadata defines industry standard XML for mashup widgets*
 - *Very close to Google Gadgets (easy to transcode with XSLT)*
 - Security
 - *OpenAjax Metadata designed to work with OpenAjax Hub 1.1 (which provides a secure mashup runtime)*

OpenAjax Metadata sample code

```
<widget xmlns="http://ns.openajax.org/widgets">  
  
  <properties>  
    <property name="Addr" type="Loc" listen="true" />  
  </properties>  
  
  <content>  
    <!-- HTML+JavaScript go here -->  
  </content>  
  
</widget>
```

OpenAjax Metadata and Google Gadgets

■ Google Gadgets

- The gorilla is the “Web Widget” space (tens of thousands of Gadgets)
- Solid technology
- However:
 - *Not a community standard*
 - *Google changes the spec without ensuring backwards compatibility*
 - *Addresses Google’s needs, which isn’t the same as everyone else’s needs*

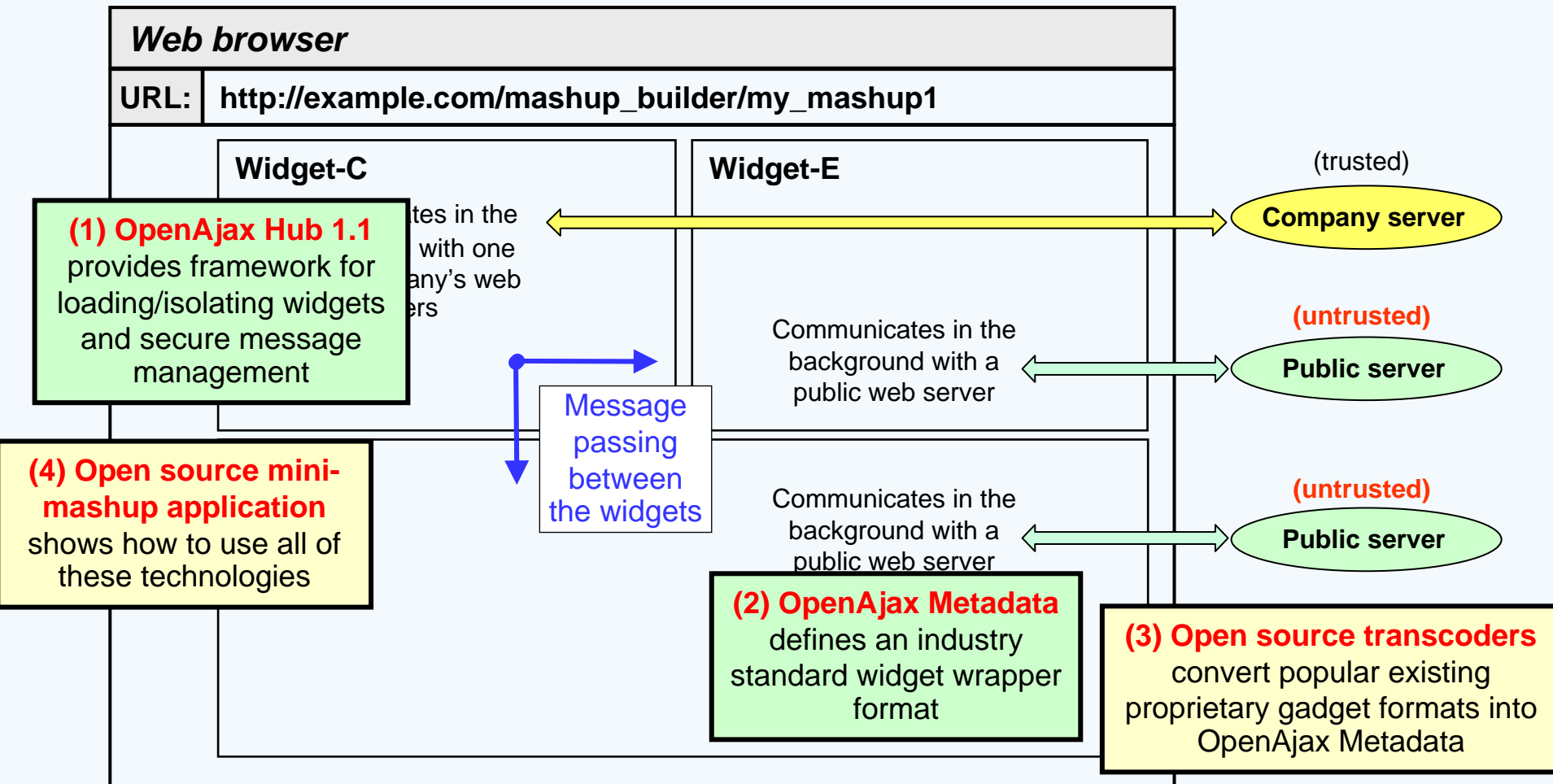
■ OpenAjax Metadata strategy

- Match Google Gadgets wherever possible
- Open source XSLT transcoders to/from Google Gadgets

OpenAjax Metadata status

- **Specification**
 - First draft spec - far along
 - http://www.openajax.org/member/wiki/OpenAjax_Metadata_Specification
- **Open source**
 - Gadget transcoders
 - Mini mashup application
- **Timeline for OpenAjax Metadata**
 - July-September 2008: 2008 InteropFest
 - Fall 2008: Finalize and approve

OpenAjax – Addressing the challenges



OpenAjax Mashups in action

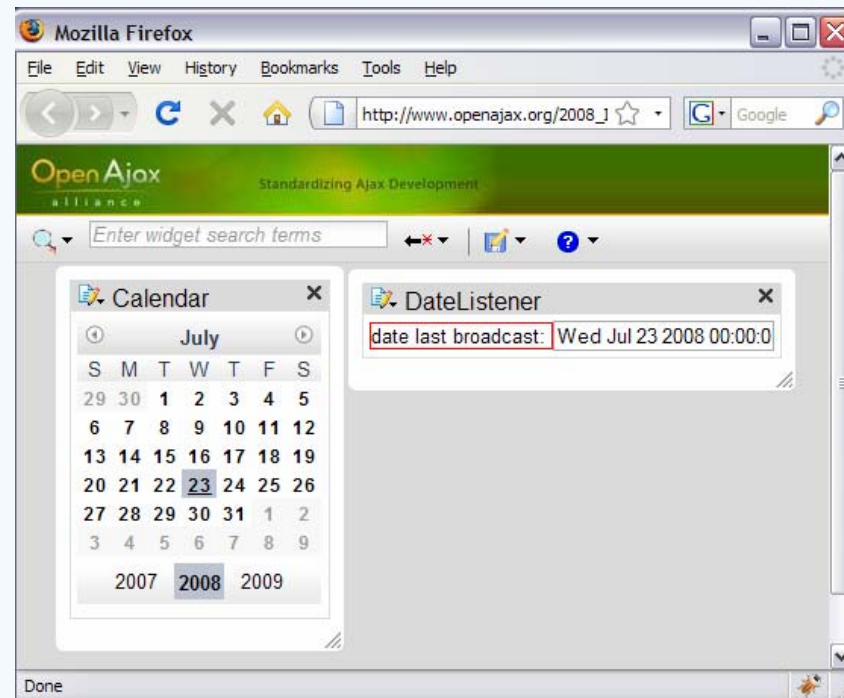
2008 InteropFest

■ Objectives

- Test OpenAjax Metadata interoperability across multiple vendors
- Test OpenAjax Hub 1.1 for reliability, performance, and suitability

■ When

- July – October, 2008



http://www.openajax.org/member/wiki/2008_InteropFest
http://www.openajax.org/2008_InteropFest/refimpl

Summary

- Mashups offer both promise, but have challenges
 - Security
 - Interoperability
- OpenAjax Alliance is addressing the challenges
 - OpenAjax Hub 1.1
 - OpenAjax Metadata

For More Information

- Web site: <http://www.openajax.org>
- Wiki: <http://www.openajax.org/member/wiki>
- Blog: <http://www.openajax.org/blog>
- Mail list: public@openajax.org
- Email: Jon Ferraiolo <jferrai@us.ibm.com>