CONSTRUCTOR UNIVERSITY

Web Service Protocols

HTTP: GET, POST, & Friends

GET Requests

- Recall: http offers
  - GET, POST, PUT, DELETE
  - …plus several more
- Request modification through key/value pairs
  - ?
  - &
- Client sends:

see REST later!

http://acme.com/srv ? mybasket=6570616275 & article=656e44204456

Request Parameters: How Passed?

- GET parameters: URL text
  - Can be cached, bookmarked
  - Reload / back in history harmless
  - Data visible in URL

```
GET srv?k1=v1&k2=v2 HTTP/1.1
```

- POST parameters: HTTP message body
  - Not cached, bookmarked
  - Reload / back in history re-submits
  - Data not visible,
    not in history,
    not in server logs

```
POST srv HTTP/1.1

k1=v1&k2=v2
```

http://www.w3schools.com/tags/ref_httpmethods.asp

REST
(Representational State Transfer)

REST

[Thomas Roy Fielding, 2002]

- REST
  = Representational State Transfer
  - Resource + URI
    - *Web = one address space*
  - representation
  - Client requests follow xlink
    - *→ new state*
- Not a standard nor product, but „architectural style“
  - = way to craft Web interface
- URI defines resource being requested
  - Consistent design philosophy
  - easy to follow
- Relies on four basic http operations:
  - GET – *Query*
  - POST – *Update*
  - PUT – *Add*
  - DELETE – *Delete*

Sample RESTful Application

- *Scenario: online shop*
- Fetch information: "shopping basket with id 5873"

GET /shoppingBasket/5873

  - Response:

```
<shoppingBasket xmlns:xlink="http://www.w3.org/1999/xlink">
   <customer xlink:href="http://shop.oio.de/customer/5873">5873</customer>
      <position nr="1" amount="5">
         <article xlink:href="http://shop.oio.de/article/4501" nr="4501">
            <description>lollypop</description>
         </article>
      </position>
   <position nr="2" amount="2">... </position>
</shoppingBasket>
```

  - Client can follow links, that changes its state
  - No side effect (status change) on server side

Sample RESTful Application (contd.)

- Place order:
  "add article #961 to shopping basket #5873"
  - Changes server state

```
POST /shoppingBasket/5873
articleNr=961
```

- Add article
  - Again, changes server state
  - Returns new id

```
PUT /article

<article>
   <description>Rooibush tea</description>
   <price>2.80</price>
   ...
</article>
```

```
HTTP/1.1 201 OK
...

http://shop.oio.de/article/6005
```

- Delete article
  - Server state change

```
DELETE /article/6005
```

Choice of Return Formats

- Propblem: how to indicate output format
  - Ex: Old browsers understood GIF, JPEG for imagery
  - GET/KVP: http://.../service-endpoint?q=...&format=image/tiff
- REST: use http Accept-Encoding parameter [IETF RFC 2616]
  - More powerful than GET: negotiate alternatives, quality factor q∈[0..1]
  - However, RESTafarians typically ignore this, use „...&f=...“ ...back to GET/KVP ;-)
- Examples:

```
Accept-Encoding: compress, gzip
Accept-Encoding:
Accept-Encoding: *
Accept-Encoding: compress;q=0.5, gzip;q=1.0
Accept-Encoding: gzip;q=1.0, identity; q=0.5, *;q=0
```

Security

- Remember: SOAP, XML-RPC do http tunneling
  - Major security leak:
    cannot determine request payload unless body is inspected and understood (!)
- REST: typed requests, firewall can judge → better security

```
hermes.oio.de - - [26/Nov/2002:12:43:07 +0100] "GET /shoppingBasket/6 HTTP/1.1" 200
hermes.oio.de - - [26/Nov/2002:12:43:08 +0100] "GET /article/12 HTTP/1.1" 200
hermes.oio.de - - [26/Nov/2002:12:43:08 +0100] "GET /article/5 HTTP/1.1" 200
hermes.oio.de - - [26/Nov/2002:12:43:09 +0100] "POST /shoppingBasket/6 HTTP/1.1" 200
hermes.oio.de - - [26/Nov/2002:12:43:13 +0100] "POST /shoppingBasket/6 HTTP/1.1" 200
hermes.oio.de - - [26/Nov/2002:12:43:14 +0100] "GET /Order/3 HTTP/1.1" 200
```

- *→ admins much more inclined to open firewall for REST services than for SOAP*

REST: How Powerful?

- Local path uses historical directory syntax → strict hierarchy

  http://.../service-endpoint/MyShop/ShoppingBaskets/14731/Article/67236

  - Standard Web servers, proxies etc can cache
- What breaks hierarchies
  - Multi-dimensional indexing – *Lat/Long/height/time has no particular sequence*
  - SQL: joins – *join tables come in no particular sequence*
  - SQL: complex predicates – *.../filter1/filter2/filter3/... cannot express AND / OR / NOT*
  - SQL: nested queries
- Remedy: old-school KVP http://.../service-endpoint/MyShop?q=*select-from-where*
  - So much more powerful, but no caching etc.

REST: Appraisal

- Strengths
  - Simple paradigm; Web = RESTful resource *(SOAP: individual spec per service)*
  - Caching *(SOAP: based on POST, not cached)*
  - Proven base stds: http, URI, MIME, XML *(SOAP: WSDL, UDDI, WS-*, BPEL, ...)*
    - *Oops: cookies break REST paradigm*
- Weaknesses
  - Assumes addressability by path + identifier (URI!) = single-root hierarchies
    → only fraction of SQL power
  - Schema to represent all URIs is complex
  - response data structure definition outside REST (*how was that with SOAP?*)
  - limited support for HTTP PUT & DELETE in popular development platforms
  - Power of http headers not accessible via browser URL

Summary

- Web services: want function invocation on server
  → Remote Procedure Call (RPC)
  - Existing since 1980s: XDR
- Web World is evolving
  - New paradigms emerging (and some disappearing)
  - GET/KVP, POST/XML, SOAP, REST, JSON, OpenAPI, ...
- Service protocol independent from database query languages!
  - Ex:
    - *GET/KVP:* http:/acme.com/access-point?q=select%20*%20from...
    - *POST/XML:* <query>select *from...</query>

AJAX
(Asynchronous Javascript and XML)

History

- Challenge: want more interactivity than "click link / reload *complete* page“
  - HTML's `iframes`
- Microsoft IE5 XMLHttpRequest object
  - Outlook Web Access, supplied with Exchange Server 2000
- 2005: term "AJAX" coined by Jesse James Garnett
- made popular in 2005 by Google Suggest
  - start typing into Google's search box → list of suggestions

AJAX

- AJAX = Asynchronous Javascript and XML
- web development technique for creating more interactive web applications
  - Goal: increase interactivity, speed, functionality, usability
  - not complete page reload → small data loads → more responsive
- asynchronous: c/s communication independent from normal page loading
  - JavaScript
  - XML
  - any server-side PL

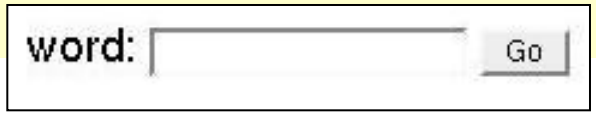
AJAX Constituent Technologies

- The core: JavaScript XMLHttpRequest object
  - Sends data, waits for response via event handler
  - Replaces <FORM> and HTTP GET / POST
- Client DOM manipulated to dynamically display & interact
  - Inject response into any place(s) of DOM tree
  - client-side scripting language: JavaScript, Jscript, ...
- Some data format
  - XML, JSON, HTML, text, ...
- Some server agent
  - Servlet, script, ...

Ajax Example: Traditional Style

- Client:

```
<form method='GET' action='http://.../ajax-ex.php'>
   word:
   <input name='wordKey' type='text'>
   <input type='submit' value='Go'>
</form>
```



- Server:

```
<?
   echo 'You have entered ' . $_GET['wordKey']
      . ' and your IP is: ' . $_SERVER['REMOTE_ADDR'];
?>
```

- Client, after page reload:

You have entered Moribundus, and your IP is: 127.0.0.1

Step 1: Avoid Complete Page Reload

```
<form name='wordForm'>
   word:
   <input name='wordKey' type='text'>
   <input type='button' value='Go' onClick='JavaScript:callBack()'>
   <div id='result'></div>
</form>
```

```
function callBack()
{  var SERVICE = 'http://.../ajax-ex.php';
   var req = new XMLHttpRequest();
   var val = document.forms['wordForm'].wordKey.value;
   req.open( 'GET', SERVICE+'?wordKey='+val, true );
   req.setRequestHeader( 'Content-Type',
                         'application/x-www-form-url
   req.send( null );
   req.onreadystatechange = function()
   {  if (req.readyState == 4)
         document.forms['wordForm'].result.innerHtml =
            req.responseText;
   }
}
```

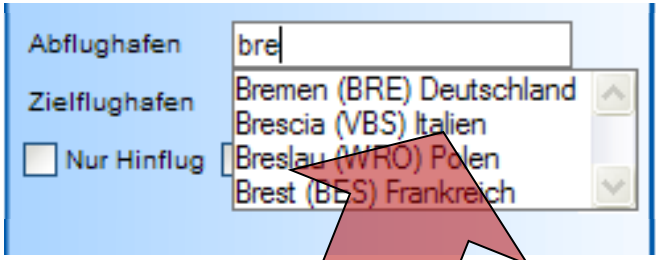
0	request not initialized
1	request set up
2	request sent
3	request in process
4	request complete

word: _____

You have entered Moribundus, and your IP is: 127.0.0.1

Step 2: Avoid SUBMIT Button

- Before: just re-implemented submit; now: allow c/s activity at any time
  - Event handlers
- Ex: suggest keywords with every char typed
  - No submit button!




```
<input name='wordKey' onKeyUp='JavaScript:callBack()'>
```

```
<? ...
   $query = "select entry from Airports
             where entry like '" . $_GET['wordKey'] . "%'";
   $result = mysql_query( $query );
   while ($row = mysql_fetch_array( $result ) )
   {
        print $row[ 'entry' ] . ",";
   }
?>
```

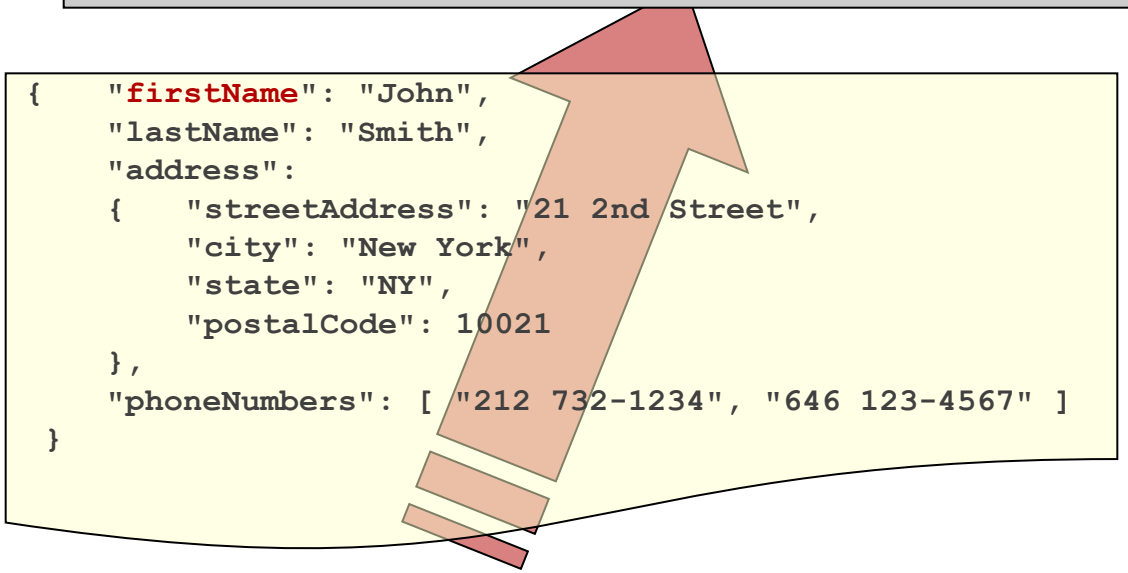
How to ship back & inject data?

Step 3: Selective Page Update

- Server sends:

```
req.onreadystatechange=function()
{   if(req.readyState==4)
    {   var p = eval( "(" + req.responseText + ")" );
        document.myForm.firstName.value = p.firstName;
    }
}
```

- JSON string sent from server:



```
{    "firstName": "John",
     "lastName": "Smith",
     "address":
     {    "streetAddress": "21 2nd Street",
          "city": "New York",
          "state": "NY",
          "postalCode": 10021
     },
     "phoneNumbers": [ "212 732-1234", "646 123-4567" ]
 }
```

- response parsing code:

```
<?  echo '{' + '"firstName":' + obj.firstName + ','
             + '"lastName":'  + obj.lastName  + ','
     … + '}'
?>
```

JSON Security Concerns

- JavaScript `eval()`
  - most JSON-formatted text is also syntactically legal JavaScript code!
  - built-in JavaScript `eval()` function executes code received
- Invitation to hack:
  embed rogue JavaScript code (server-side attack),
  intercept JSON data evaluation (client-side attack)
  - Safe alternative: `parseJSON()` method,
    see ECMAScript v4 and www.json.org/json.js
- Cross-site request forgery
  - malicious page can request & obtain JSON data belonging to another site

AJAX / JSON Portability

- AJAX uses standardized components, supported by all major browsers:
  - JavaScript, XML, HTML, CSS
- XMLHttpRequest object part of std DOM
  - Windows: ActiveX control Msxml2.XMLHTTP (IE5), Microsoft.XMLHTTP (IE6)
- ...similarly for JSON

Sample Tool Support: jQuery

- JavaScript library, http://jquery.com
- Code examples:

```
$( "button.continue" ).html( "Next Step..." )
```

```
$.ajax({
  url: "/api/getWeather",
  data: {
    zipcode: 97201
  },
  success: function( data ) {
    $( "#weather-temp" ).html( "<b>" + data + "</b> degrees" );
  }
});
```

Appraisal: AJAX Advantages

- Reduced bandwidth usage
  - No complete reload/redraw, HTML generated locally, only actual data transferred
    → payload coming down much smaller in size
  - Can load stubs of event handlers, then functions on the fly
- Separation of data, format, style, and function
  - encourages programmers to clearly separate methods & formats:

Raw data / content	→ normally embedded in XML
webpage	→ HTML / XHTML
web page style elements	→ CSS
Functionality	→ JavaScript + XMLHttp + server code

Appraisal: AJAX Disadvantages

- **Browser integration**
  - dynamically created page not registered in browser history
  - bookmarks
- **Search engine optimization**
  - Indexing of Ajax page contents?
  - (not specific to Ajax, same issue with all dynamic data sites)
- **Web analytics**
  - Tracking of accessing page vs portion of page vs click?
- **Response time concerns from network latency**
  - Web transfer hidden → effects from delays sometimes difficult to understand for users
- **Reliance on JavaScript**
  - JavaScript compatibility issue → blows up code; Remedy: libraries such as `prototype`
  - IDE support used to be poor, changing
  - Can switch off JavaScript in my browser
- **Security**
  - Can fiddle with data getting into browser

Summary

- AJAX allows to add desktop flavour to web apps
  - JSON as lightweight, fast alternative to XML
- Web programming paradigm based on existing, available standards
- Issues: browser compatibility, security, web dynamics
- Manifold usages:
  - real-time form data validation; autocompletion; bg load on demand; sophisticated user interface controls and effects (trees, menus, data tables, rich text editors, calendars, progress bars, ...); partial submit; mashups (app mixing); desktop-like web app

AJAX
(Asynchronous Javascript and XML)

History

- Challenge: want more interactivity than "click link / reload *complete* page“
  - HTML's `iframes`
- Microsoft IE5 XMLHttpRequest object
  - Outlook Web Access, supplied with Exchange Server 2000
- 2005: term "AJAX" coined by Jesse James Garnett
- made popular in 2005 by Google Suggest
  - start typing into Google's search box → list of suggestions

AJAX

- AJAX = Asynchronous Javascript and XML
- web development technique for creating more interactive web applications
  - Goal: increase interactivity, speed, functionality, usability
  - not complete page reload → small data loads → more responsive
- asynchronous: c/s communication independent from normal page loading
  - JavaScript
  - XML
  - any server-side PL

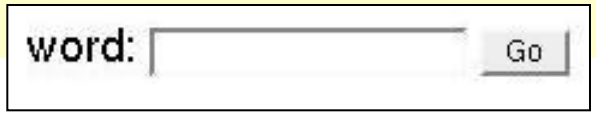
Constituent Technologies

- The core: JavaScript XMLHttpRequest object
  - Sends data, waits for response via event handler
  - Replaces <FORM> and HTTP GET / POST
- Client DOM manipulated to dynamically display & interact
  - Inject response into any place(s) of DOM tree
  - client-side scripting language: JavaScript, Jscript, ...
- Some data format
  - XML, JSON, HTML, text, ...
- Some server agent
  - Servlet, script, ...

Ajax Example: Traditional Style

- Client:

```
<form method='GET' action='http://.../ajax-ex.php'>
   word:
   <input name='wordKey' type='text'>
   <input type='submit' value='Go'>
</form>
```



- Server:

```
<?
   echo 'You have entered ' . $_GET['wordKey']
      . ' and your IP is: ' . $_SERVER['REMOTE_ADDR'];
?>
```

- Client, after page reload:

You have entered Moribundus, and your IP is: 127.0.0.1

Step 1: Avoid Complete Page Reload

```
<form name='wordForm'>
   word:
   <input name='wordKey' type='text'>
   <input type='button' value='Go' onClick='JavaScript:callBack()'>
   <div id='result'></div>
</form>
```

```
function callBack()
{  var SERVICE = 'http://.../ajax-ex.php';
   var req = new XMLHttpRequest();
   var val = document.forms['wordForm'].wordKey.value;
   req.open( 'GET', SERVICE+'?wordKey='+val, true );
   req.setRequestHeader( 'Content-Type',
                         'application/x-www-form-url
   req.send( null );
   req.onreadystatechange = function()
   {  if (req.readyState == 4)
         document.forms['wordForm'].result.innerHtml =
            req.responseText;
   }
}
```

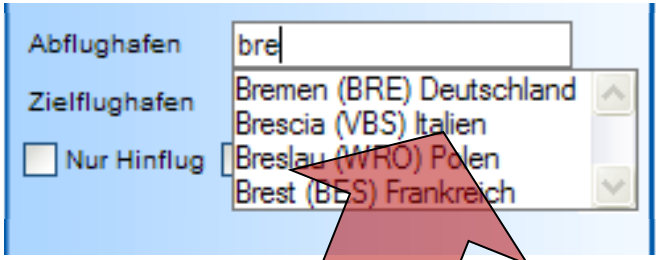
0	request not initialized
1	request set up
2	request sent
3	request in process
4	request complete

word: _____

You have entered Moribundus, and your IP is: 127.0.0.1

Step 2: Avoid SUBMIT Button

- Before: just re-implemented submit; now: allow c/s activity at any time
  - Event handlers
- Ex: suggest keywords with every char typed
  - No submit button!




```
<input name='wordKey' onKeyUp='JavaScript:callBack()'>
```

```
<? ...
   $query = "select entry from Airports
             where entry like '" . $_GET['wordKey'] . "%'";
   $result = mysql_query( $query );
   while ($row = mysql_fetch_array( $result ) )
   {
        print $row[ 'entry' ] . ",";
   }
?>
```

How to ship back & inject data?

JSON

- JSON = JavaScript Object Notation
  - Lightweight data interchange format
  - MIME type: **`application/json`** (RFC 4627)
  - text-based, human-readable
- alternative to XML use
  - Subset of JavaScript's object literal notation
  - 10x faster than XML parsing
  - _way_ easier to handle
  - JSON parsing / generating code readily available for many languages

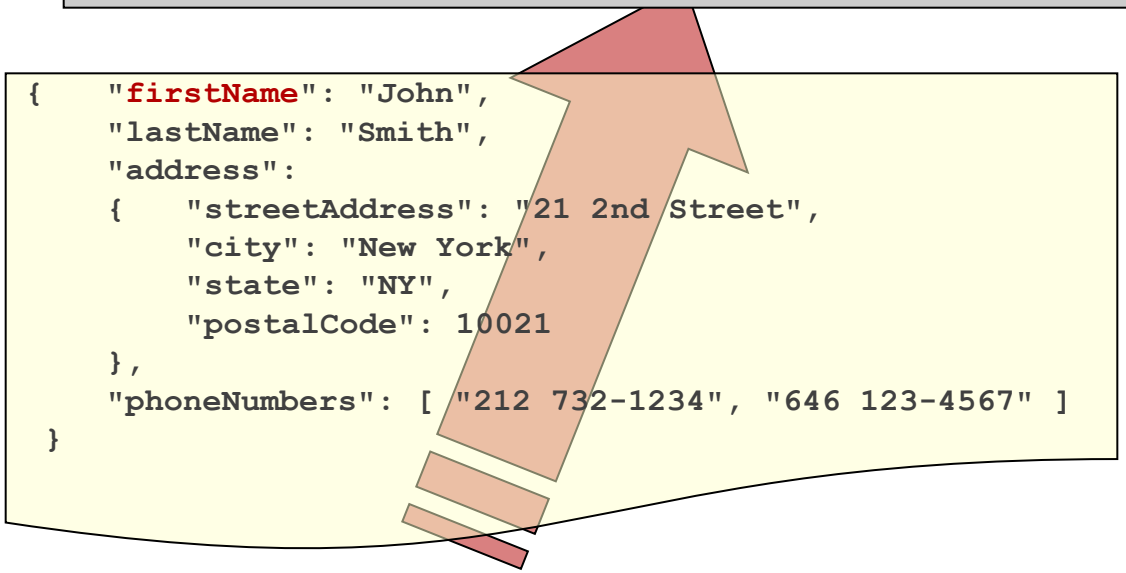
"JSON is XML without garbage"

JSON Example

- Server sends:

```
req.onreadystatechange=function()
{   if(req.readyState==4)
    {   var p = eval( "(" + req.responseText + ")" );
        document.myForm.firstName.value = p.firstName;
    }
}
```

- JSON string sent from server:



```
{    "firstName": "John",
     "lastName": "Smith",
     "address":
     {    "streetAddress": "21 2nd Street",
          "city": "New York",
          "state": "NY",
          "postalCode": 10021
     },
     "phoneNumbers": [ "212 732-1234", "646 123-4567" ]
 }
```

- response parsing code:

```
<?  echo '{' + '"firstName":' + obj.firstName + ','
             + '"lastName":'  + obj.lastName  + ','
     … + '}'
?>
```

JSON Security Concerns

- JavaScript `eval()`
  - most JSON-formatted text is also syntactically legal JavaScript code!
  - built-in JavaScript `eval()` function executes code received
- Invitation to hack:
  embed rogue JavaScript code (server-side attack),
  intercept JSON data evaluation (client-side attack)
  - Safe alternative: `parseJSON()` method,
    see ECMAScript v4 and www.json.org/json.js
- Cross-site request forgery
  - malicious page can request & obtain JSON data belonging to another site

AJAX / JSON Portability

- AJAX uses standardized components, supported by all major browsers:
  - JavaScript, XML, HTML, CSS
- XMLHttpRequest object part of std DOM
  - Windows: ActiveX control Msxml2.XMLHTTP (IE5), Microsoft.XMLHTTP (IE6)
- ...similarly for JSON

Appraisal: AJAX Advantages

- Reduced bandwidth usage
  - No complete reload/redraw, HTML generated locally, only actual data transferred
    → payload coming down much smaller in size
  - Can load stubs of event handlers, then functions on the fly
- Separation of data, format, style, and function
  - encourages programmers to clearly separate methods & formats:

Raw data / content	→ normally embedded in XML
webpage	→ HTML / XHTML
web page style elements	→ CSS
Functionality	→ JavaScript + XMLHttp + server code

Appraisal: AJAX Disadvantages

- **Browser integration**
  - dynamically created page not registered in browser history
  - bookmarks
- **Search engine optimization**
  - Indexing of Ajax page contents?
  - (not specific to Ajax, same issue with all dynamic data sites)
- **Web analytics**
  - Tracking of accessing page vs portion of page vs click?
- **Response time concerns from network latency**
  - Web transfer hidden → effects from delays sometimes difficult to understand for users
- **Reliance on JavaScript**
  - JavaScript compatibility issue → blows up code; Remedy: libraries such as `prototype`
  - IDE support used to be poor, changing
  - Can switch off JavaScript in my browser
- **Security**
  - Can fiddle with data getting into browser

Tool Support: Examples

- jQuery, http://jquery.com/

```
$( "button.continue" ).html( "Next Step..." )
```

- AJAX:

```
$.ajax({
  url: "/api/getWeather",
  data: {
    zipcode: 97201
  },
  success: function( data ) {
    $( "#weather-temp" ).html( "<b>" + data + "</b> degrees" );
  }
});
```

Kore rawa e rawaka te reo kotahi