

The Complete Reference

Includes an Ajax
communication
library

Ajax

- ★ Design, debug, and manage highly interactive Ajax applications
- ★ Ensure Ajax application availability, speed, and security with best practices
- ★ Explore emerging ideas such as Comet, Web Services, and Offline Access

Thomas A. Powell

**Mc
Graw
Osborne**

Contents

Acknowledgments	xv
Introduction	xvii

Part I Core Ideas

1 Introduction to Ajax	3
Ajax Defined	3
Hello Ajax World	5
The Challenges of Running Ajax Examples Locally	11
The Rise of Ajax	12
Implications of Ajax	13
Summary	14
2 Pre-Ajax JavaScript Communications Techniques	15
One-way Communication	15
One-way Image Object Technique	18
One-way Iframes with Query Strings	22
One-way Script Tags	22
Other Approaches	23
One-way Iframes with Form Posts	23
Cookie-based Transport	30
Two-way Communications	32
Images for Two-way Communications	32
Two-way Script Tag Communication	39
Less Common Two-way Methods	40
Two-way Iframes	42
Communications Pattern Review	49
Example Applications	50
A Client-Side JS Error Reporter	50
Offsite Link Press Monitoring	52
Fancy Ratings—Pre-Ajax Version	55
RSS Reader	58
Summary	59
3 XMLHttpRequest Object	61
Overview of XHRs	61
Instantiation and Cross-Browser Concerns	64
ActiveX XHR Anxiety	64
A Cross-Browser XHR Wrapper	73

XHR Request Basics	74
Synchronous Requests	74
Asynchronous Requests	77
Sending Data via GET	79
Sending Data via Post	81
Request Headers	82
Other HTTP Requests	84
Head Requests	84
Response Basics	86
readyState Revisited	86
status and statusText	90
responseText	92
responseXML	92
Response Headers	97
Controlling Requests	97
Authentication with XHRs	99
Propriety and Emerging XHR Features	101
Managing MIME Types	102
Multipart Responses	103
onProgress and Partial Responses	105
Other Firefox Event Handlers	107
XHR Arcana and Future Changes	108
XHR Implications and Challenges	108
Ajax and Memory Leaks	110
Summary	114
4 Data Formats	115
Ajax and Character Sets	115
Data Format Decisions	118
Encoding/Decoding Requests	119
Encoding/Decoding Responses	119
Security Considerations	120
Transmission Considerations	120
Standard Encoding: x-www-form-urlencoded	121
Extending Standard Encoding	122
Form Serialization	126
Object Serialization	128
Using Other Input Formats	129
XML	129
JSON	132
Other Request Forms: YAML, Text, and Beyond	136
File Attachments	142
Response Formats	146
Text Responses	146
Script Responses	150

XML Responses and Handling	152
Well-Formed XML	154
Valid XML	155
XML and the DOM	157
Processing Responses with XPath	160
Transforming Responses with XSLT	163
Data Islands: Proprietary and Powerful	167
Binary Responses	169
Encoded Content: Base64	169
Experimenting with Data URLs	171
File Responses	173
Summary	173

Part II Applied Ajax

5 Developing an Ajax Library	177
Not Another Ajax Library!	177
AjaxTCR Library Overview	179
Adding Modern Conveniences	186
Data Format Handling	189
Request Status	190
Request Control	193
AjaxTCR Library Utility Functions	194
AjaxTCR Library Basic Features Summary	196
Beyond the AjaxTCR Library	200
Introduction to YUI	201
YUI's Connection Manager	202
Other YUI Features	211
Introduction to Prototype	211
Ajax Prototype Style	212
Prototype Ajax Assistance	217
Exploring Prototype Further	220
Introduction to jQuery	223
jQuery's Approach to Ajax	223
jQuery Ajax Conveniences	227
The Strengths and Weaknesses of jQuery	228
Other Libraries: Dojo and Beyond	229
Summary	230
6 Networking Considerations	231
What Could Go Wrong?	231
Timeouts	232
Retries	233
Handling Server Errors	235
Handling Content Errors	238

Dealing with Multiple Requests	241
Beyond the Two-Connection Limit?	243
Request Queues	245
Order Is Not Guaranteed	250
Are Race Conditions Possible?	254
Ensuring Communication Robustness	256
Server Availability	256
Client Availability	257
Connection Rates	257
Tracking Network Conditions	258
Improving Ajax Performance	261
HTTP Compression	261
Content Optimization	264
Caching	270
Busting Browser Caches	270
Working with the Browser Cache	272
An Ajax Response Cache	273
Precaching	275
Get the Balance Right	276
There's Always More	279
Summary	281
7 Security Concerns	283
The Web Attack Surfaces	283
Web Application Reconnaissance Review	285
Web Application Attack Review	287
Ajax Security Differences	293
JavaScript Security	294
JavaScript Protection	294
JavaScript's Security Policy	298
Same-Origin Policy	298
Exceptions to the Same-Origin Policy	300
Trusted External Scripts	301
Ajax and Authentication	301
HTTP Authentication under Ajax	302
Ajax and SSL	308
Custom Form-Cookie Authentication	310
Cross-Site Scripting	312
Addressing XSS	314
XHR Hijacking with XSS	316
History Exposure: The Start of a Hack	320
Cross Site Request Forgery (CSRF)	322
CSRF Attacks on JSON, JSONP and Script Responses	324
Defeating CSRF	327
Ajax Payload Protection	328

Web Services and Ajax: Security's Pandora's Box	331
Summary	334
8 User Interface Design for Ajax	335
The User Interface Implications of Ajax	335
Communicating Network Activity	337
Traditional Web Pattern Activity Indicators	337
Ajax Application's Activity Indicators	340
Detailed Status Indications	342
Communicating Problems and Errors	348
Communicating Change	352
To-Do List Introduction: Delete, Confirm, and Transition	355
Patterns of Immediacy	359
Click-to-Edit	360
Click-to-Edit List	365
Drag-and-Drop	367
Draggable List	373
The Real Power: Data on Demand	377
Auto Completion and Suggestion	378
Auto Search	384
Auto Validation	386
Previewing	394
Progressive Loading	395
The Danger of Incremental Loading	399
What About...?	400
Putting Things Together	401
Accessibility	403
Summary	405
9 Site and Application Architecture with Ajax	407
Adding Ajax	407
In-Page Ajax	411
Rating Refactored	412
Building a Rating Widget	413
Enabling Alternate Transports	418
Automatic Communication Fallback	425
Degrading Not Enhancing	427
Leveraging Templates	430
Client-Side Templates	434
Applied Templates	442
Wrapping the Widget	445
Full-Site Ajax	451
Fighting the Back Button Blues	452
Embracing History	458
Applied History	467
Ajax and Bookmarking	473

A Full Example: To-Do List	474
Coupled or Decoupled Architecture	476
Loose Coupling	476
Tight Coupling	476
Exploring Tightly Coupled Architecture Approaches	477
Architectural Final Analysis	479
Summary	479

Part III Advanced Topics

10 Web Services and Beyond	483
Ajax and Web Services	483
Server Proxy Solution	485
URL Forwarding Scheme	490
Using the <script> Tag	492
Flash Cross Domain Bridge	496
The Future: Native XHR Cross Domain Access	500
SOAP: All Washed Up?	502
Screen Scraping	505
Sampling Public Services	508
Mash-ups	511
Comet	514
Polling: Fast or Long	518
The Long Slow Load	520
Binary Socket Bridget	523
Server Event Listeners	526
The Comet Challenge: Web Chat	527
The Comet Impact	528
Going Offline	529
Client Persistence and Storage	529
Danger: Offline Ahead!	535
Enabling Offline with Google Gears	537
Emerging Offline Possibilities with Firefox 3	545
Summary	548

Part IV Appendixes

A JavaScript Quick Reference	551
Language Fundamentals	551
Language Versions and Conformance	552
JavaScript Inclusion Methods	554
Data Types	556
Primitive Types	556
Type Conversion	557

Composite Types	559
ECMAScript Built-In Objects	562
Identifiers	565
Reserved Words	566
Variables	567
Variable Scope	567
Operators	568
Arithmetic Operators	569
Bitwise Operators	569
Assignment Operators	569
Logical Operators	571
Conditional Operator	571
Type Operators	571
Comma Operator	572
Relational Operators	573
Operator Precedence and Associativity	574
Statements and Blocks	575
Conditional Statements	576
Loops	577
Object Iteration	578
JavaScript 1.7's Generators and Iterators	578
Functions	579
The with Statement	581
Exceptions	581
Regular Expressions	582
Comments	583
B HTTP 1.1 Reference	587
HTTP Requests	587
HTTP Methods	588
HTTP Headers	589
General Headers	590
Entity Headers	590
Request Headers	591
HTTP Responses	597
Response Headers	602
MIME	605
C AjaxTCR Library Reference	609
Coding Conventions Used	609
AjaxTCR.comm	610
Request Options Object Properties	610
Request Object Instance Properties	619
AjaxTCR.comm.cache	620
AjaxTCR.comm.cookie	620

AjaxTCR.comm.stats	620
AjaxTCR.data	620
AjaxTCR.history	620
AjaxTCR.storage	620
AjaxTCR.template	622
AjaxTCR.util.DOM	622
AjaxTCR.util.event	632
AjaxTCR.util.misc	632
Index	635