

HTTP and HTTPS – What Every Web Developer Needs to Know

John C. Flack

Synectics for Management Decisions, Inc.

It All Starts with a Request





Lou Costello

Bud Abbott



Request and Response

- HTTP and HTTPS are Stateless
 - Each Request is Independent
 - Each Response too
 - Any state is an illusion
 - JEE – the Java standard for web applications creates a session id and stores it in a cookie
 - Apex does the same
 - If your web dev platform doesn't, then you must code it.
 - Even then – when does a session end?
-
-

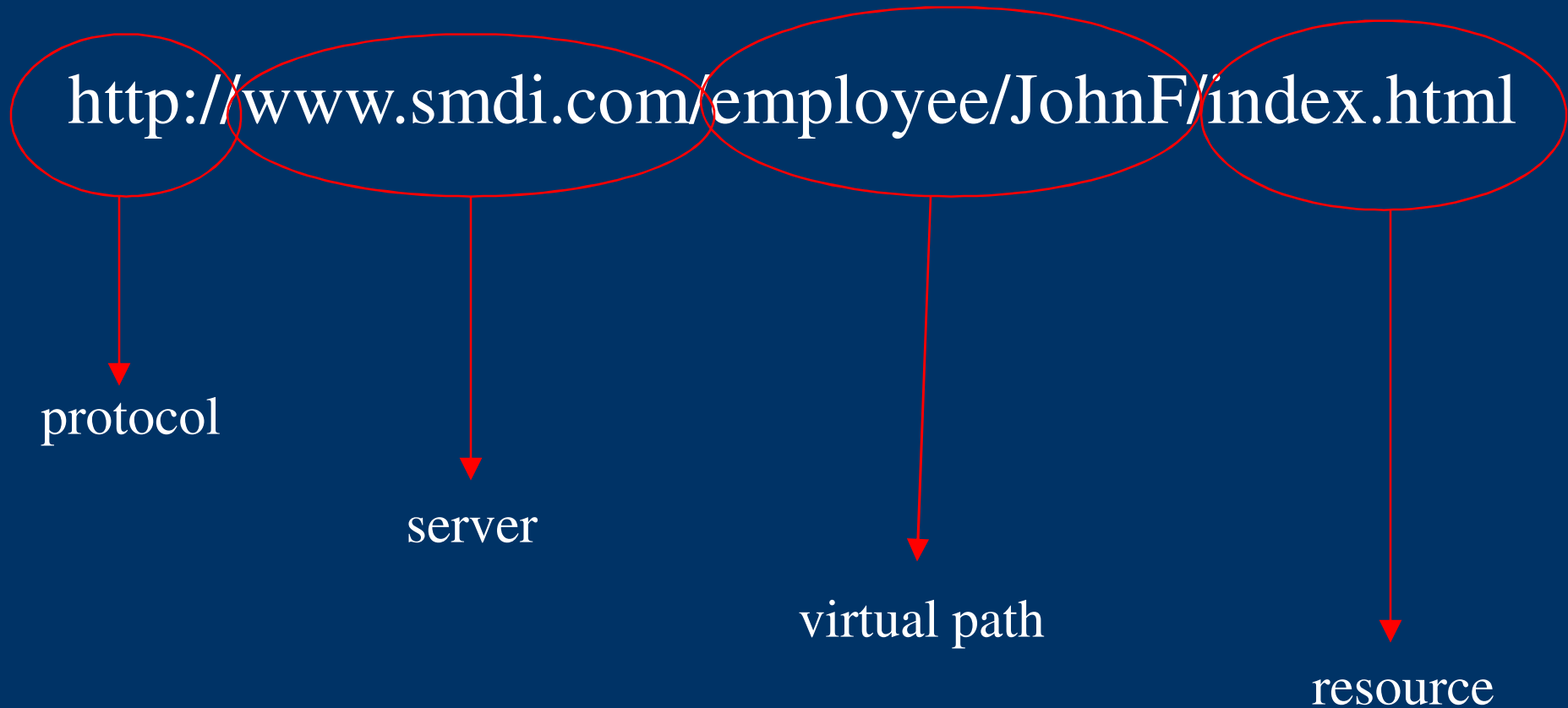
Types of Requests

- GET – the original and still most common
 - Images
 - Javascript scripts
 - CSS Stylesheets
 - REST web services
 - Other resources referenced on a web page
 - POST
 - Data filled in on HTML Forms
 - Uploaded Files
 - SOAP web services
-
-

WebDAV

- Request types
 - PUT
 - MOVE
 - COPY
 - LOCK
 - Two from Oracle
 - OraDAV
 - XMLDB
- ... But we're not going to talk about these
-
-

Dissecting an URL



Environment Variables

DOCUMENT_ROOT	The root directory of your server
HTTP_COOKIE	The visitor's cookie, if one is set
HTTP_HOST	The hostname of the page being attempted
HTTP_REFERER	The URL of the page that called your program
HTTP_USER_AGENT	The browser type of the visitor
HTTPS	on if the program is being called through a secure server
PATH	The system path your server is running under
QUERY_STRING	The query string (see GET, below)
REMOTE_ADDR	The IP address of the visitor
REMOTE_HOST	The hostname of the visitor (if your server has reverse-name-lookups on; otherwise this is the IP address again)
REMOTE_PORT	The port the visitor is connected to on the web server
REMOTE_USER	The visitor's username (for .htaccess-protected pages)

Environment Variables (cont.)

REQUEST_METHOD	GET or POST
REQUEST_URI	The interpreted pathname of the requested document or CGI (relative to the document root)
SCRIPT_FILENAME	The full pathname of the current CGI
SCRIPT_NAME	The interpreted pathname of the current CGI (relative to the document root)
SERVER_ADMIN	The email address for your server's webmaster
SERVER_NAME	Your server's fully qualified domain name (e.g. www.cgi101.com)
SERVER_PORT	The port number your server is listening on
SERVER_SOFTWARE	The server software you're using (e.g. Apache 1.3)

Who Are You?

The Place of Authentication in the
Protocol.





Basic and Digest Authentication

Authentication Required

A username and password are being requested by <http://buprenorphine.samhsa.gov>. The site says: "bwms_private"

User Name:

Password:

OK Cancel

The Problem with Basic Authentication



Form Based Authentication

Single Sign On - Login - Mozilla Firefox

File Edit View History Bookmarks Tools Help

oracle.com https://login.oracle.com/myso/signon.jsp?site2pstoretoken=v1.2~9F7227A3~A3DEDBD052C4

Most Visited Getting Started Latest Headlines HOME - Comcast.net Metro - Trip Planner

Single Sign On - Login

ORACLE.COM TECHNOLOGY NETWORK PARTNERS STORE SUPPORT

ORACLE

Sign In

Enter your Single Sign-On user name and password.

Username

Password

[Lost Password?](#)
[Need Login Help?](#)

Why Sign In?

Sign in to access premium content and advanced functions.

- Manage subscriptions and newsletters.
- Access downloads, discussion forums and social networks.
- Use applications from anywhere, anytime.

[Create your Oracle account now.](#)

By creating an account, you acknowledge and agree to the [Terms of Use](#) concerning your access to and use of the Oracle Web site and the services and content provided on the Oracle Web site, and our [Privacy Policy](#). Read them carefully before you finish creating your account.

Copyright © 2010, Oracle. All rights reserved.

About Oracle | Contact Us | Site Maps | Legal Notices and Terms for Use | Privacy Statement
Powered by Oracle Application Server Portal

This site is intended solely for use by Oracle's authorized users. Use of this site is subject to the Legal Notices, Terms for Use and Privacy Statement located on this site. Use of the site by customers and partners, if authorized, is also subject to the terms of your contract(s) with Oracle. Use of this site by Oracle employees is also subject to company policies, including the Code of Conduct. Unauthorized access or breach of these terms may result in termination of your authorization to use this site and/or civil and criminal penalties.

Done

Public/Private Key Encryption

- If it was Encrypted with my Public Key
 - It can only be Decrypted with my Private Key
 - If I keep my Private Key secret, only I can read it.
 - If it was Encrypted with my Private Key
 - It can only be Decrypted with my Public Key
 - So, you Know only I could have sent the message.
-
-

But How do I Know that this is Your Public Key?



About HTTPS

- AKA Secure Sockets Layer (SSL)
 - Now Known as Transport Layer Security (TLS)
 - Public/Private Key Based
 - Like Client Certificate Authentication
 - Server Provides Certificate
 - All Requests/Responses are Encrypted
 - Performance
 - Often only part of the site uses HTTPS
-
-

Content Type

What are you sending me?



Header Lines in Response

SERVER_ADMIN	The email address for your server's webmaster
SERVER_NAME	Your server's fully qualified domain name (e.g. www.cgi101.com)
SERVER_PORT	The port number your server is listening on
SERVER_SOFTWARE	The server software you're using (e.g. Apache 1.3)
SET-COOKIE	Saves a cookie on the user's browser
CONTENT-TYPE	Identifies the type of data in the response



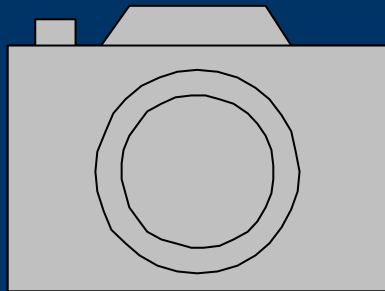
MIME



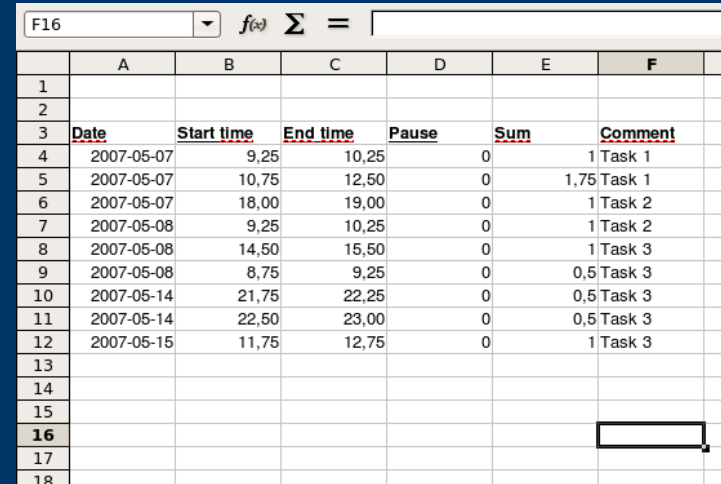
Multipurpose Internet Mail Extensions (MIME)



text/html



image/jpeg



	A	B	C	D	E	F
1						
2						
3	Date	Start time	End time	Pause	Sum	Comment
4	2007-05-07	9,25	10,25	0	1	Task 1
5	2007-05-07	10,75	12,50	0	1,75	Task 1
6	2007-05-07	18,00	19,00	0	1	Task 2
7	2007-05-08	9,25	10,25	0	1	Task 2
8	2007-05-08	14,50	15,50	0	1	Task 3
9	2007-05-08	8,75	9,25	0	0,5	Task 3
10	2007-05-14	21,75	22,25	0	0,5	Task 3
11	2007-05-14	22,50	23,00	0	0,5	Task 3
12	2007-05-15	11,75	12,75	0	1	Task 3
13						
14						
15						
16						
17						
18						

application/vnd.ms-excel



text/css

POST and MIME

- Form Fields
 - Sent as an attachment to the request
 - Yes, just like an e-mail attachment
 - MIME Type of Form Fields
 - application/x-www-form-urlencoded
 - But for File Uploads
 - multipart/form-data
 - Done with the enctype attribute of FORM element in HTML
 - Says that there is more than one attachment
-
-

From Inside the Browser



From the Server



Conclusions

- HTTP and HTTPS are stateless
 - Request/Response
 - Pass information besides query strings and form data
 - Call authentication
 - HTTPS encrypts
 - Files are attached like e-mail
-
-

About the Speaker

- Address:
Synectics for Management Decisions, Inc.
1901 N. Moore St.
Arlington, VA 22209
 - E-Mail
 - JohnF@smdi.com
 - Web Site
 - <http://www.smdi.com/employee/JohnF/>
 - Blog
 - <http://it.toolbox.com/blogs/jjflash-oracle-journal/>
-
-