Glossary

This glossary defines some of the common terminology related to Apache in particular, and web serving in general. More information on each concept is provided in the links.

Definitions

Access Control
The restriction of access to network realms. In an Apache context usually the restriction of access to certain *URLs*.
See: Authentication, Authorization, and Access Control

Algorithm
An unambiguous formula or set of rules for solving a problem in a finite number of steps. Algorithms for encryption are usually called *Ciphers*.

APache eXtension Tool (apxs)
A perl script that aids in compiling module sources into Dynamic Shared Objects (DSOs) and helps install them in the Apache Web server.
See: Manual Page: apxs

Apache Portable Runtime (APR)
A set of libraries providing many of the basic interfaces between the server and the operating system. APR is developed parallel to the Apache HTTP Server as an independent project.
See: Apache Portable Runtime Project

Authentication
The positive identification of a network entity such as a server, a client, or a user.
See: Authentication, Authorization, and Access Control

Certificate
A data record used for authenticating network entities such as a server or a client. A certificate contains X.509 information pieces about its owner (called the subject) and the signing Certification Authority (called the issuer), plus the owner's public key and the signature made by the CA. Network entities verify these signatures using CA certificates.
See: SSL/TLS Encryption

Certificate Signing Request (CSR)
An unsigned certificate for submission to a Certification Authority, which signs it with the Private Key of their CA *Certificate*. Once the CSR is signed, it becomes a real certificate.
See: SSL/TLS Encryption

Certification Authority (CA)
A trusted third party whose purpose is to sign certificates for network entities it has authenticated using secure means. Other network entities can check the signature to verify that a CA has authenticated the bearer of a certificate.
See: SSL/TLS Encryption

Cipher
An algorithm or system for data encryption. Examples are DES, IDEA, RC4, etc.
See: SSL/TLS Encryption

Ciphertext
The result after Plaintext is passed through a Cipher.
See: SSL/TLS Encryption

Common Gateway Interface (CGI)
A standard definition for an interface between a web server and an external program that allows the external program to service requests. There is an Informational RFC which covers the specifics.
See: Dynamic Content with CGI

Configuration Directive
See: Directive

Configuration File

A text file containing Directives that control the configuration of Apache.
See: Configuration Files

CONNECT
An HTTP method for proxying raw data channels over HTTP. It can be used to encapsulate other protocols, such as the SSL protocol.

Context
An area in the configuration files where certain types of directives are allowed.
See: Terms Used to Describe Apache Directives

Digital Signature
An encrypted text block that validates a certificate or other file. A Certification Authority creates a signature by generating a hash of the *Public Key* embedded in a *Certificate*, then encrypting the hash with its own *Private Key*. Only the CA's public key can decrypt the signature, verifying that the CA has authenticated the network entity that owns the *Certificate*.
See: SSL/TLS Encryption

Directive
A configuration command that controls one or more aspects of Apache's behavior. Directives are placed in the Configuration File
See: Directive Index

Dynamic Shared Object (DSO)
Modules compiled separately from the Apache `httpd` binary that can be loaded on-demand.
See: Dynamic Shared Object Support

Environment Variable (env-variable)
Named variables managed by the operating system shell and used to store information and communicate between programs. Apache also contains internal variables that are referred to as environment variables, but are stored in internal Apache structures, rather than in the shell environment.
See: Environment Variables in Apache

Export-Crippled
Diminished in cryptographic strength (and security) in order to comply with the United States' Export Administration Regulations (EAR). Export-crippled cryptographic software is limited to a small key size, resulting in *Ciphertext* which usually can be decrypted by brute force.
See: SSL/TLS Encryption

Filter
A process that is applied to data that is sent or received by the server. Input filters process data sent by the client to the server, while output filters process documents on the server before they are sent to the client. For example, the `INCLUDES` output filter processes documents for Server Side Includes.
See: Filters

Fully-Qualified Domain-Name (FQDN)
The unique name of a network entity, consisting of a hostname and a domain name that can resolve to an IP address. For example, `www` is a hostname, `example.com` is a domain name, and `www.example.com` is a fully-qualified domain name.

Handler
An internal Apache representation of the action to be performed when a file is called. Generally, files have implicit handlers, based on the file type. Normally, all files are simply served by the server, but certain file types are "handled" separately. For example, the `cgi-script` handler designates files to be processed as CGIs.
See: Apache's Handler Use

Hash
A mathematical one-way, irreversible algorithm generating a string with fixed-length from another string of any length. Different input strings will usually produce different hashes (depending on the hash function).

Header
The part of the HTTP request and response that is sent before the actual content, and that contains meta-information describing the content.

.htaccess
A configuration file that is placed inside the web tree and applies configuration directives to the directory where it is placed and all sub-directories. Despite its name, this file can hold almost any type of directive, not just access-control directives.
See: Configuration Files

httpd.conf
: The main Apache configuration file. The default location is `/usr/local/apache2/conf/httpd.conf`, but it may be moved using run-time or compile-time configuration.
See: Configuration Files

HyperText Transfer Protocol (HTTP)
: The standard transmission protocol used on the World Wide Web. Apache implements version 1.1 of the protocol, referred to as HTTP/1.1 and defined by RFC 2616.

HTTPS
: The HyperText Transfer Protocol (Secure), the standard encrypted communication mechanism on the World Wide Web. This is actually just HTTP over SSL.
See: SSL/TLS Encryption

Method
: In the context of HTTP, an action to perform on a resource, specified on the request line by the client. Some of the methods available in HTTP are `GET`, `POST`, and `PUT`.

Message Digest
: A hash of a message, which can be used to verify that the contents of the message have not been altered in transit.
See: SSL/TLS Encryption

MIME-type
: A way to describe the kind of document being transmitted. Its name comes from that fact that its format is borrowed from the Multipurpose Internet Mail Extensions. It consists of a major type and a minor type, separated by a slash. Some examples are `text/html`, `image/gif`, and `application/octet-stream`. In HTTP, the MIME-type is transmitted in the `Content-Type` header.
See: mod_mime

Module
: An independent part of a program. Much of Apache's functionality is contained in modules that you can choose to include or exclude. Modules that are compiled into the Apache `httpd` binary are called *static modules*, while modules that are stored separately and can be optionally loaded at run-time are called *dynamic modules* or DSOs. Modules that are included by default are called *base modules*. Many modules are available for Apache that are not distributed as part of the Apache HTTP Server tarball. These are referred to as *third-party modules*.
See: Module Index

Module Magic Number (MMN)
: Module Magic Number is a constant defined in the Apache source code that is associated with binary compatibility of modules. It is changed when internal Apache structures, function calls and other significant parts of API change in such a way that binary compatibility cannot be guaranteed any more. On MMN change, all third party modules have to be at least recompiled, sometimes even slightly changed in order to work with the new version of Apache.

OpenSSL
: The Open Source toolkit for SSL/TLS
See http://www.openssl.org/#

Pass Phrase
: The word or phrase that protects private key files. It prevents unauthorized users from encrypting them. Usually it's just the secret encryption/decryption key used for Ciphers.
See: SSL/TLS Encryption

Plaintext
: The unencrypted text.

Private Key
: The secret key in a Public Key Cryptography system, used to decrypt incoming messages and sign outgoing ones.
See: SSL/TLS Encryption

Proxy
: An intermediate server that sits between the client and the *origin server*. It accepts requests from clients, transmits those requests on to the origin server, and then returns the response from the origin server to the client. If several clients request the same content, the proxy can deliver that content from its cache, rather than requesting it from the origin server each time, thereby reducing response time.
See: mod_proxy

Public Key
: The publicly available key in a Public Key Cryptography system, used to encrypt messages bound for its owner and to decrypt signatures made by its owner.
See: SSL/TLS Encryption

Public Key Cryptography
: The study and application of asymmetric encryption systems, which use one key for encryption and another for decryption. A corresponding pair of such keys constitutes a key pair. Also called Asymmetric Cryptography.
See: SSL/TLS Encryption

Regular Expression (Regex)
: A way of describing a pattern in text - for example, "all the words that begin with the letter A" or "every 10-digit phone number" or even "Every sentence with two commas in it, and no capital letter Q". Regular expressions are useful in Apache because they let you apply certain attributes against collections of files or resources in very flexible ways - for example, all .gif and .jpg files under any "images" directory could be written as "`/images/.*(jpg|gif)$`". In places where regular expressions are used to replace strings, the special variables $1 ... $9 contain backreferences to the grouped parts (in parentheses) of the matched expression. The special variable $0 contains a backreference to the whole matched expression. To write a literal dollar sign in a replacement string, it can be escaped with a backslash. Historically, the variable & could be used as alias for $0 in some places. This is no longer possible since version 2.3.6. Apache uses Perl Compatible Regular Expressions provided by the PCRE library. You can find more documentation about PCRE's regular expression syntax at that site, or at Wikipedia.

Reverse Proxy
: A proxy server that appears to the client as if it is an *origin server*. This is useful to hide the real origin server from the client for security reasons, or to load balance.

Secure Sockets Layer (SSL)
: A protocol created by Netscape Communications Corporation for general communication authentication and encryption over TCP/IP networks. The most popular usage is *HTTPS*, i.e. the HyperText Transfer Protocol (HTTP) over SSL.
See: SSL/TLS Encryption

Server Name Indication (SNI)
: An SSL function that allows passing the desired server hostname in the initial SSL handshake message, so that the web server can select the correct virtual host configuration to use in processing the SSL handshake. It was added to SSL starting with the TLS extensions, RFC 3546.
See: the SSL FAQ and RFC 3546

Server Side Includes (SSI)
: A technique for embedding processing directives inside HTML files.
See: Introduction to Server Side Includes

Session
: The context information of a communication in general.

SSLeay
: The original SSL/TLS implementation library developed by Eric A. Young

Subrequest
: Apache provides a subrequest API to modules that allows other filesystem or URL paths to be partially or fully evaluated by the server. Example consumers of this API are `DirectoryIndex`, `mod_autoindex`, and `mod_include`.

Symmetric Cryptography
: The study and application of *Ciphers* that use a single secret key for both encryption and decryption operations.
See: SSL/TLS Encryption

Tarball
: A package of files gathered together using the `tar` utility. Apache distributions are stored in compressed tar archives or using pkzip.

Transport Layer Security (TLS)
: The successor protocol to SSL, created by the Internet Engineering Task Force (IETF) for general communication authentication and encryption over TCP/IP networks. TLS version 1 is nearly identical with SSL version 3.
See: SSL/TLS Encryption

Uniform Resource Locator (URL)

The name/address of a resource on the Internet. This is the common informal term for what is formally called a Uniform Resource Identifier. URLs are usually made up of a scheme, like `http` or `https`, a hostname, and a path. A URL for this page might be `http://httpd.apache.org/docs/trunk/glossary.html`.

Uniform Resource Identifier (URI)

A compact string of characters for identifying an abstract or physical resource. It is formally defined by RFC 2396. URIs used on the world-wide web are commonly referred to as URLs.

Virtual Hosting

Serving multiple websites using a single instance of Apache. *IP virtual hosting* differentiates between websites based on their IP address, while *name-based virtual hosting* uses only the name of the host and can therefore host many sites on the same IP address.
See: Apache Virtual Host documentation

X.509

An authentication certificate scheme recommended by the International Telecommunication Union (ITU-T) which is used for SSL/TLS authentication.
See: SSL/TLS Encryption