安全的 HTTP (SSL/TLS) 服务会将 Web 浏览器与 Web 服务器之间的通讯数据进行加密, 如果您的服务器运行着关键的应用, 或若您的 Web 页面需要用户输入那些需保密的信息, 使用安全的 HTTP 服务是必须的.

以下是对如何针对 Apache Web 服务器设置安全的 HTTP 服务的简单介绍, 可能不同的操作系统上其做法会有所不同, 但基本原理是一致的.

所需的软件:

- apache2 (Web 服务器)
- openssl

1: 创建一个自行签发证书:

首先, 您需要创建一个服务器密钥,

openssl genrsa -aes256 -out server-sec.key 4096

…以及证书签发请求 (CSR)

openssl req -new -key server-sec.key -out server.csr

之后, 将其用服务器密钥进行签发以生成服务器证书

openssl x509 -req -days 3650 -in server.csr -signkey server-sec.key -out server.crt

将 server-sec.key 文件放在一个安全的地方, 并将其访问许可设置成只有超级用户可读写. 然后生成一个无口令保护的密钥供 Web 服务器.

openssl rsa -in server-sec.key -out server.key

至此, 您应该有了以下支持文件:

- server.key (Apache 用的无口令保护密钥)
- server.csr (证书签发请求)
- server.crt (证书)
- server-sec.key (服务器密钥)

2: 更新 Apache Web 服务器的 SSL 配置

找出您机器上的 Apache Web 服务器的配置目录. 对于 Apache 2.x 版本, 它可能在 /etc/httpd/conf.d

为 ssl.conf 文件作一备份:

cp ssl.conf ssl.conf.ORIG

然后, 对 ssl.conf 文件进行编辑, 找出'<VirtualHost *:443>' 并将其配置改成与以下类似:

<VirtualHost *:443>

ServerName ServerName

DocumentRoot /var/www-ssl/html/

接着, 在同一文件中, 找到以 'SSLCertificateFile'开头,和以'SSLCertificateKeyFile'开头的行, 例如, 在 RHEL 6.3 上, 有如下两行:

SSLCertificateFile /etc/pki/tls/certs/localhost.crt

SSLCertificateKeyFile /etc/pki/tls/private/localhost.key

用先前生成的 'server.key' 和 'server.crt' 来取代这二个文件:

SSLCertificateFile /etc/pki/tls/certs/ServerName.crt

SSLCertificateKeyFile /etc/pki/tls/private/ServerName.key

cp server.crt /etc/pki/tls/certs/ServerName.crt

cp server.key /etc/pki/tls/private/ServerName.key

之后, 重新起动 Web 服务器.

注: 本文档是经由修改由互联网上所得到的资料而得的, 特此感谢原有资料的作者.