SSL VERSION

There are several versions of the SSL protocol defined. The latest version, the Transport Layer Security Protocol (TLS), is based on SSL 3.0

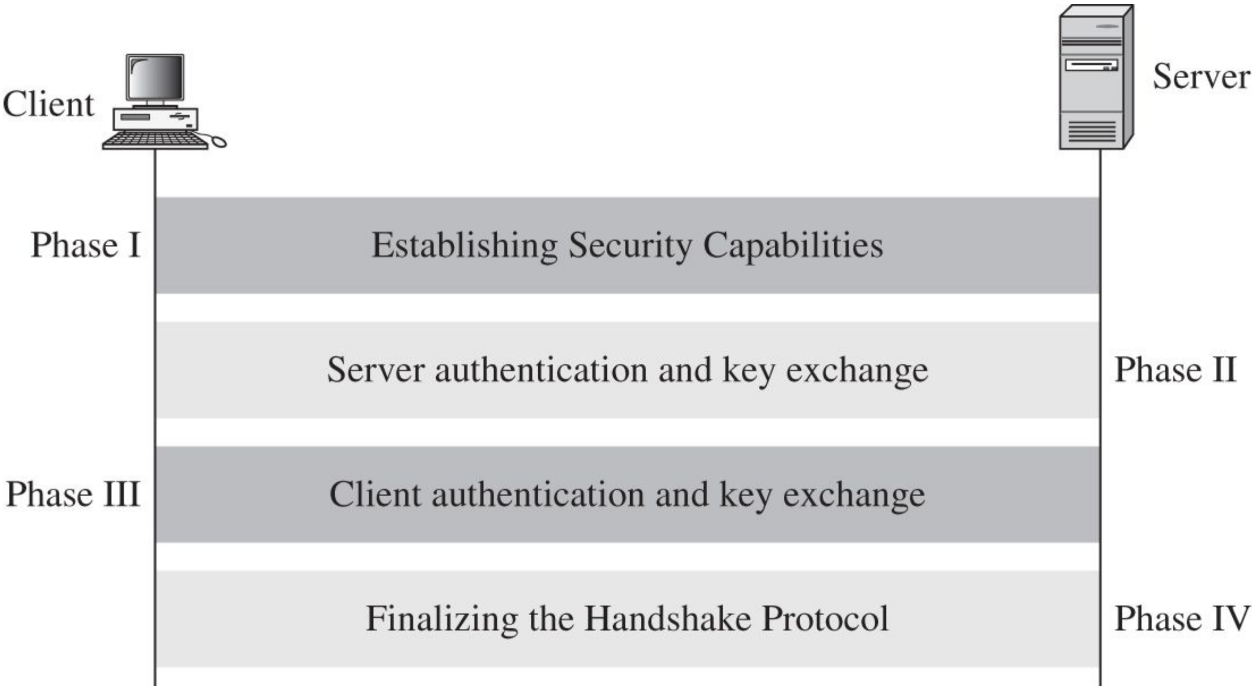
SSL Version 1.0

SSL Version 2.0

SSL Version 3.0

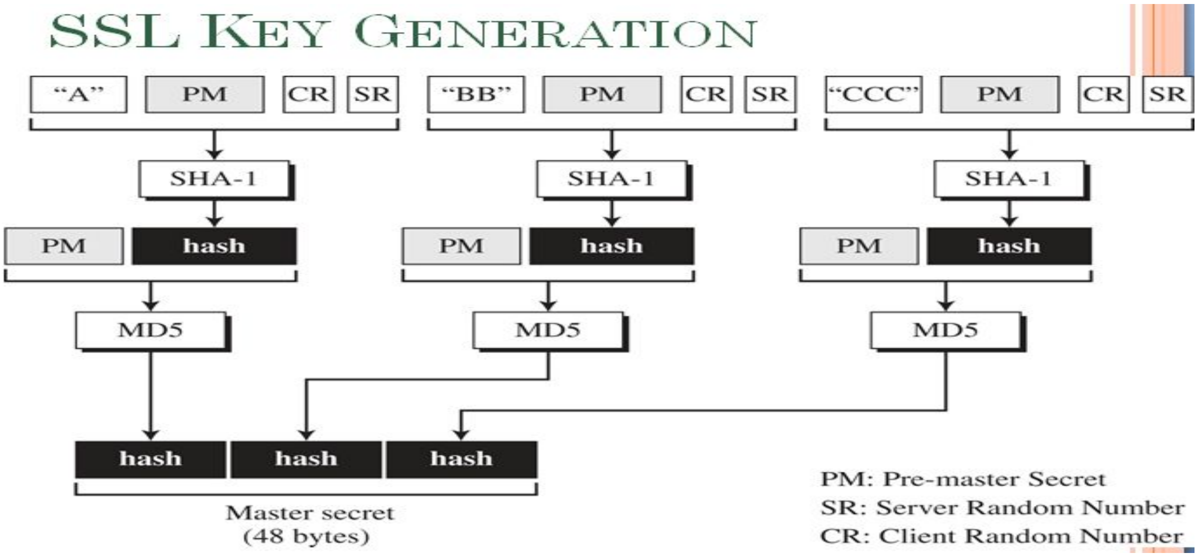
TLS Version 1.0
TLS Version 1.0 with SSL Version 3.0 compatibility

Secure Socket Layer Protocol


Client
Server
Phase I
Establishing Security Capabilities
Server authentication and key exchange
Phase II
Phase III
Client authentication and key exchange
Finalizing the Handshake Protocol
Phase IV

Finalization handshakes prottocol (Sender signs/encrypts "finished" message Receiver decrypts/verifies message to confirm keys)

The SSL handshake is a complicated process that involves significant cryptographic key exchanges. However, the handshake can be completed by calling SSL_accept() on the SSL server and SSL_connect() on the SSL client.



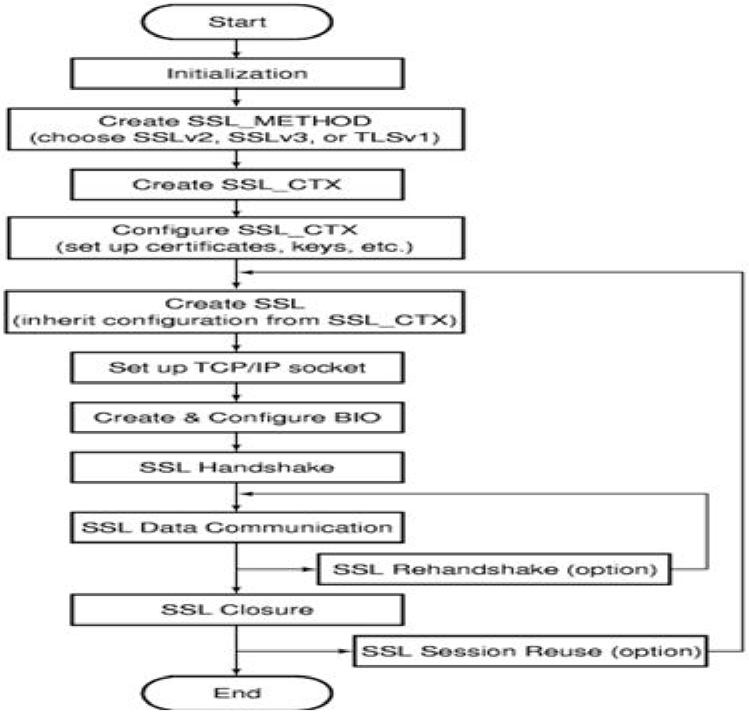
Client and server use to generate <u>master key</u> used to create cipher keys

<u>ALGORITHM USED:</u>

- **DES.** Data Encryption Standard, an encryption algorithm used by the U.S. Government.
- **DSA.** Digital Signature Algorithm, part of the digital authentication standard used by the U.S. Government.
- **KEA.** Key Exchange Algorithm, an algorithm used for key exchange by the U.S. Government.
- **MD5.** Message Digest algorithm developed by Rivest.
- **RC2 and RC4**. Rivest encryption ciphers developed for RSA Data Security.
- **RSA.** A public-key algorithm for both encryption and authentication. Developed by Rivest, Shamir, and Adleman.
- **RSA key exchange.** A key-exchange algorithm for SSL based on the RSA algorithm.
- **SHA-1.** Secure Hash Algorithm, a hash function used by the U.S. Government.
- **SKIPJACK.** A classified symmetric-key algorithm implemented in FORTEZZA-compliant hardware used by the U.S. Government. (For more information, see FORTEZZA Cipher Suites.)

Triple-DES. DES applied three times

Overview of SSL Application with OpenSSL APIs


Start
Initialization
Create SSL_METHOD
(choose SSLv2, SSLv3, or TLSv1)
Create SSL_CTX
Configure SSL_CTX
(set up certificates, keys, etc.)
Create SSL
(inherit configuration from SSL_CTX)
Set up TCP/IP socket
Create & Configure BIO
SSL Handshake
SSL Data Communication
SSL Rehandshake (option)
SSL Closure
SSL Session Reuse (option)
End