OpenSSL

Creation of keys and self-assigned certificates, widely used in projects using secure communication

Process – Creation of private key server, followed by generating a certificate-signing request. Certificate-signing request is signed using the server’s private key

“OpenSSL used for creating certificates”, 2015 [Online]. Available: - <https://openssl.org>

Transport Layer Security (TLS)

* Contains a set of cryptographic protocols designed to provide communication security over a computer network
* Goal – Provide privacy & data integrity between two computer communication applications
* Two Layers – TLS Handshake Protocol & TLS Record Protocol
* Handshake deals with verification process & key exchange
* Record deals with encryption & Sending of data

Example

1. The client sends a “Client Hello” message to the server.
2. The server responds with a “Server Hello”.
3. The server sends its certificate message.
4. After verification of certificate, the client encrypts a session key using the server’s public key.
5. The server receives the session key and decrypts it using its private key. This is based on the asymmetric RSA algorithm.
6. Now both the client and the server have the session key. Data will now be sent through AES-128 based symmetric key encryption.
7. Client sends “Client Hello Done”.
8. Server also sends “Server Hello Done”.
9. Handshake protocol is completed.

C. Meyer, “20 Years of SSL/TLS Research, An Analyis of the Internet’s Security Foundation”, Doktor-Ingenieur, Ruhr-University Bochum, Feb. 2014

T. Jager, F. Kohlar, S. Schäge, and J. Schwenk, "On the security of TLS-DHE in the standard model," Advances in Cryptology –CRYPTO 2012. vol. 7417, pp. 273–293, Aug 2012.

RSA Algorithm

* Public-private key based asymmetric form of encryption
* Public key available to everyone & anyone can encrypt data & send to that key
* Data can only be decrypted using individuals private key
* Used to send session key from client to server

N. Y. Goshwe, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment," International Journal of Computer Science and Network Security, vol. 13, no. 7, pp. 9–13, Jul. 2013.

AES Algorithm

* Advanced Encryption Standard
* Symmetric form of encryption, same key is used for encryption as well as decryption
* Rasp Pi mentioned project uses 128 bit AES key

Creation of self-signed certificate - Self-signed certificates were created using OpenSSL in the terminal on the computer. This involved three steps as follows:

* Generating Server Private Key. The key size was kept at 2048 bits.
* Generating Certificate Signing Request (CSR) containing server information and public key of server. The IP address of the server is saved in the configuration file along with other information such as address and contact details of the server for identity verification purposes.
* Self-signing the certificate with the Server’s private key. In reality a third party Certification Authority does this after verification of server details

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7785011>

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8328710>