Assignment 4

Abbas Khan , Mariia Rybalka , Linara Adilova

June 4, 2016

Task 4.4 (theoretical): TLS Cipher Suites

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

ECDHE - Cipher suites using authenticated ephemeral ECDH key agreement. the client and server will agree on encryption keys using Ephemeral Elliptic Curve Diffie-Hellman. RSA - Cipher suites using RSA key exchange, authentication or either respectively. the client will verify that the key is valid using the RSA algorithm to communications. AES128 GCM - cipher suites using 128 bit AES. AES in Galois Counter Mode (GCM). the actual encryption of my web browsing session will be performed SHA256 - Ciphersuites using SHA256. the SHA algorithm will be used for securely hashing parts of the TLS messages.

1. Authentication
2. Encryption
3. Integrity

TLS RSA RC4 128 MD5
[1]

References

[1] Not forget *http://www.welivesecurity.com/2015/02/05/alternatives-passwords/* WeLiveSecurity by ESET