Secure and Dependable Systems
Jacobs University Bremen
Huzaifa Hashim

Course: CO21-320203
April 21th, 2020

SADS Problem Set 8

Problem 8.1

Pretty Good Privacy
Solution:
a) Write down the sum of your matriculation number and 139626885.

$$\begin{array}{cccccccccc} & 1 & 3 & 9 & 6 & 2 & 6 & 8 & 8 & 5 \\ + & & 3 & 0 & 0 & 0 & 1 & 9 & 2 & 8 \\ \hline & 1 & 6 & 9 & 6 & 2 & 8 & 8 & 1 & 3 \end{array}$$

b) What is the purpose of a PGP revocation certificate?

A PGP revocation certificate is generated to invalidate a key-pair in case of breach of security or if one loses their secret key. This certificate is uploaded onto the server which lets people know who are using the key of the revocation such that no data is encrypted using this key anymore. The certificate should be created with GPG when a key is being generated since it cannot be done without possession of both the private key and the passphrase. This allows the owner to have the control to revoke their key.

Problem 8.2

Transport Layer Security (TLS 1.2)
Solution:

a) What is the Pseudorandom Function (PRF)?

The pseudorandom function (PRF) in TLS 1.2 is used to create the Master Secret. It is also a source of entropy when creating session keys for TLS 1.2. It takes as input three parameters, the label, the secret and the seed and is then used to compute a securely generated pseudo-random output of arbitrary length.

b) TLS has a notion of a pre-master secret and a master secret. Explain why both exist and how they relate to each other and the key exchange algorithm negotiated between the two TLS peers.

TLS 1.2 works with the notion of symmetric encryption algorithms since they are more efficient. The pre-master secret is the essential part of this encryption scheme, where the PRF is fed this pre-master secret, with a series of random values to generate a master secret. After the generation of the master secret which is 48 bytes long, the pre-master secret is discarded, and the master secret is used to derive symmetric keys for encryption and decryption. The fail safe mechanism in TLS 1.2 is the deletion of the pre-master secret, which makes it more robust to hackers since the pre-master secret is not used after the master secret has been generated which is then in turn used to generate symmetric keys, application data can be encrypted using the agreed upon symmetric encryption algorithms.

c) How are keys used by the symmetric encryption algorithms derived from the master secret?

After a handshake protocol is established, TLS 1.2 uses the PRF to create key material from the master secret. The master secret is passed to the PRF with the label ”key expansion”. This forms a sequence of secure bytes which are split into the encryption and MAC keys for both the server and client.

Problem 8.3

Transport Layer Security (TLS 1.3)

Solution:

a) Summarize how the HMAC-based Extract-and-Expand Key Derivation Function (HDKF) works.

HMAC-based Extract-and-Expand Key Derivation Function (HKDF) works on the extract-expand paradigm. It first extracts a pseudorandom key using an HMAC hash function which takes in an optional salt which is non-secretive and input keying material. This function produces a key, the length of which is denoted by the hash function, e.g SHA-256.

It then uses the output of this hash function and turns it into the output keying material by repeatedly appending it to the output key material and then truncating the key to the desired length which is specified in the expand function.

b) How are keys used by the symmetric encryption algorithms derived from the master secret?

After a handshake protocol is established, TLS uses the HKDF-Extract and Derive-Secret functions to derive the keys. To add a new Input Keying Material, HKDF-Extract is used with the current secret state.

References:

1. https://tools.ietf.org/html/rfc8446page-145