CS6740: Network Security Anoop Pai

Algorithms used:

Symmetric key encryption (AES) is used for encrypting plain-text as it is much faster than Asymmetric key encryption; especially when a huge amount of data is involved. However, I have used asymmetric key encryption (RSA) for encrypting the shared session key which is used during symmetric encryption. In addition, public key encryption is much more secure in comparison, as private key is only present with the receiver who decrypts the message. Also, as the sender knows just the receiver's public key, it is not sufficient to decrypt the given message.

I've used RSA to digitally sign the message using the sender's private key. During this process, I ensure that padding was used with OAEP using receiver's public key. This was done as RSA is not resilient to cipher text attacks. By using OAEP, we can ensure that RSA is secure. Furthermore, SHA256 has been used internally which acts as a good means of one-way hashing.

The usage of HMAC is to make sure the integrity of the message is preserved. In order to verify the integrity of received message, the sender digitally makes a signature on the HMAC of the plaintext which was obtained using the public key and the message. Plus, as the session key is required for HMAC, those users who can verify the signature to obtain the HMAC are able to obtain the HMAC.

Justification for using AES:

One of the reason for going with AES over, say, DES is that the 128 bits used in AES makes it more secure vs 64 bits in DES. Therefore, going with larger sizes of keys adds to the security. Some other reasons for using AES vs other symmetric approach like 3DES is as follows:

- AES key size 128/192/256 vs 3DES 116/168/56.
- 3DES is slow as it runs DES thrice on the various keys
- AES is known for using a single strong key, where 3DES uses encryption keys repeatedly

In addition to the above points, AES is prominently used and is renowned to be very resilient to attacks when the key and IV are chosen wisely.

CTR Mode

The approach implemented in this program involves a AES-256 with CTR mode. CTR mode, basically, converts block cipher into stream cipher and provides good security, given we generate different pseudo random number generated for the same key. As the key generated is of size 256 bits and IV is half of that (128), there is a 2^128 chance that the same none would be selected for every key.

As IV is factored into our encryption, AES provides a greater sense of security.

No additional padding is necessary in the case of CTR mode as it is resilient to padding oracle attacks. The reason HMAC + CTR has been used over GCM for integrity is because CTR with HMAC uses two keys as a measure of authentication whereas GCM uses the randomly generated key for authentication.

As mentioned before, the usage of 256 bits (Key size) in AES ensures that the nonce and key pair in the CTR mode are of variable length which reduces the chances of the none and the key being the same. Lastly, the nonce size of CTR mode must be the same as the block size of AES which is 128 bits. (AES IV)